IFIP AICT 684

Deepak Puthal
Saraju Mohanty
Baek-Young Choi (Eds.)

Internet of Things

Advances in Information and Communication Technology

6th IFIP International Cross-Domain Conference, IFIPIoT 2023
Denton, TX, USA, November 2–3, 2023
Proceedings, Part II

2 Part II

Springer

ifip 60 YEARS

IFIP IoT

IFIP Advances in Information and Communication Technology 684

IFIP Advances in Information and Communication Technology

The IFIP AICT series publishes state-of-the-art results in the sciences and technologies of information and communication. The scope of the series includes: foundations of computer science; software theory and practice; education; computer applications in technology; communication systems; systems modeling and optimization; information systems; ICT and society; computer systems technology; security and protection in information processing systems; artificial intelligence; and human-computer interaction.

Edited volumes and proceedings of refereed international conferences in computer science and interdisciplinary fields are featured. These results often precede journal publication and represent the most current research.

The principal aim of the IFIP AICT series is to encourage education and the dissemination and exchange of information about all aspects of computing.

More information about this series at https://link.springer.com/bookseries/6102

Deepak Puthal · Saraju Mohanty ·
Baek-Young Choi
Editors

Internet of Things

Advances in Information and Communication Technology

6th IFIP International Cross-Domain Conference, IFIPIoT 2023
Denton, TX, USA, November 2–3, 2023
Proceedings, Part II

Springer

Editors
Deepak Puthal
Khalifa University
Abu Dhabi, United Arab Emirates

Saraju Mohanty
University of North Texas
Denton, TX, USA

Baek-Young Choi
University of Missouri at Kansas City
Kansas City, MO, USA

ISSN 1868-4238 ISSN 1868-422X (electronic)
IFIP Advances in Information and Communication Technology
ISBN 978-3-031-45881-1 ISBN 978-3-031-45882-8 (eBook)
https://doi.org/10.1007/978-3-031-45882-8

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Paper in this product is recyclable.

Preface

6th IFIP International Conference on Internet of Things (IFIP IoT 2023)

The rapid evolution of technology has led to the development of the Internet of Things (IoT), a network of physical objects that are embedded with sensors, software, and network connectivity, enabling them to collect and exchange data. The IoT is transforming our digital landscape, and the IFIP Internet of Things (IFIP-IoT) 2023 conference is a crucial platform for scholars, researchers, and practitioners to come together, share ideas, and advance this transformative field.

This edited book is a compilation of cutting-edge research and developments presented at the IFIP-IoT conference. The conference serves as a dynamic hub where experts from diverse backgrounds come together to explore the multifaceted aspects of IoT, from its technological foundations to its far-reaching implications for society, industry, and beyond.

The chapters in this book are a testament to the collaborative spirit of the IFIP-IoT community. They offer insights into the latest innovations, challenges, and opportunities in IoT, covering a wide array of topics, including IoT architectures, security and privacy, data analytics, edge computing, and applications in various domains. These contributions not only reflect the state of the art in IoT research but also provide valuable perspectives that pave the way for future breakthroughs.

The IFIP-IoT Conference is an annual IFIP event dedicated to IoT research, innovation, and applications, emphasizing the multidisciplinary nature of IoT. IoT encompasses topics from network protocols and embedded systems to analytics, machine learning, and social, legal, ethical, and economic considerations, enabling services in e-health, mobility, energy, manufacturing, smart cities, agriculture, and more. Security, privacy, and societal aspects are essential in IoT deployment. IFIP-IoT covers these diverse areas, seeking papers showcasing technical advancements, research, innovation, pilot results, and policy discussions. Contributors include researchers, users, organizations, ICT industry experts, authorities, and regulators.

IFIP-IoT welcomed full and short paper submissions, with full papers being original and unpublished elsewhere. Poster presentations were limited to student papers. The conference program featured keynotes, plenary talks, tutorials, technical sessions, special sessions, expert panels, a research demo session (RDS), and a student research forum (SRF). New tracks like “SRF” and “RDS” aimed to enhance event participation.

The paper submission guidelines include an 18-page limit for full papers, which applied to both regular and special sessions, as well as an 8-page limit for short papers, applicable to any session, including SRF and RDS. To ensure a thorough review process, we implemented a four-tier review mechanism within EDAS, consisting of TPC-Chairs, Track Chairs, TPC members, and dedicated reviewers. We took measures to address conflicts of interest by appointing multiple TPC chairs and multiple track chairs for each track. Additionally, we imposed a limit of 2 papers maximum for PC members. SRF encouraged student first-author papers with an 8-page limit, while RDS papers also had an 8-page limit and may or may not feature student first authors. It's important to note that TPC members were permitted to co-author papers with their students in both SRF and RDS. Furthermore, our conference included Regular tracks/ sessions that accept submissions from any authors, as well as Special Sessions/Tracks proposed by established researchers, with submissions received by invitation.

The IFIP-IoT conference had six regular tracks, each focusing on a different aspect of IoT:

- **Hardware/Software Solutions for IoT and CPS (HSS):** This track covered the design, development, and implementation of hardware and software solutions for IoT and cyber-physical systems (CPS).
- **Electronics and Signal Processing for IoT (ESP):** This track focused on the use of electronics and signal processing techniques for IoT applications.
- **Artificial Intelligence and Machine Learning Technologies for IoT (AMT):** This track explored the use of artificial intelligence (AI) and machine learning (ML) technologies for IoT applications.
- **Cyber Security/Privacy/Trust for IoT and CPS (SPT):** This track addressed the security, privacy, and trust challenges of IoT and CPS systems.
- **IoT or CPS Applications and Use Cases (APP):** This track presented case studies and applications of IoT and CPS technologies.
- **Networking and Communications Technology for IoT (NCT):** This track focused on the networking and communication technologies used in IoT systems.

Leading IoT experts from around the globe proposed special sessions on cutting-edge IoT topics. These session organizers then invited other established researchers to submit papers to their sessions. We are pleased to announce that the following special sessions took place and contributed excellent research papers to the IFIP-IoT 2023 conference:

- **AI and Big Data for Next-G Internet of Medical Things (IoMT):** This special session explored the use of AI and big data for the next generation of IoMT systems.
- **Blockchain for IoT-Driven Systems (BIoT):** This special session examined the use of blockchain for IoT-driven systems.
- **Edge AI for Smart Wearables (EAW):** This special session focused on the use of edge AI for smart wearables.
- **Energy-Aware Security for IoT (EAS):** This special session addressed the security challenges of IoT systems, with a focus on energy efficiency.
- **IoT for Smart Healthcare (SHC):** This special session explored the use of IoT for smart healthcare applications.
- **IoT for Wearables and Smart Devices (IWS):** This special session focused on the use of IoT for wearables and smart devices.
- **Metaverse for IoT (MIoT):** This special session examined the use of the metaverse for IoT applications.

- **Security by Design for IoT (SbD):** This special session discussed the importance of security by design for IoT systems.
- **Technologies for Smart Agriculture (TSA):** This special session explored the use of IoT technologies for smart agriculture.

In addition to the regular tracks and special sessions mentioned earlier, we introduced two sessions to support graduate students, early career researchers, and ongoing projects through short papers:

- **Student Research Forum (SRF):** This session was designed to provide valuable opportunities for research scholars and graduate students. Presentations in this session were in a concise oral or poster format.
- **Research Demo Session (RDS):** Authors in this session had the chance to showcase live demonstrations and hardware prototypes of their research.

We are grateful to the authors who contributed their expertise to this volume, and we commend their dedication to advancing the field of IoT. We would also like to acknowledge the reviewers whose insightful feedback ensured the quality and rigor of the included chapters.

We hope that this edited book will serve as a valuable resource for researchers, educators, policymakers, and industry professionals alike, fostering a deeper understanding of IoT and inspiring further innovation in this transformative domain. As the IFIP-IoT conference continues to evolve and grow, we look forward to witnessing the continued impact of this vibrant community on the ever-expanding Internet of Things.

Deepak Puthal
Saraju Mohanty
Baek-Young Choi

Organization

General Chairs

Saraju Mohanty	University of North Texas, USA
Shengli Fu	University of North Texas, USA

Program Chairs

Baek-Young Choi	University of Missouri Kansas City, USA
Deepak Puthal	Khalifa University, UAE
Carlos Pereira	Federal University of Rio Grande do Sul, Brazil

Publication Chairs

Hui Zhao	University of North Texas, USA
Sharad Sharma	University of North Texas, USA

Web Chairs

Laavanya Rachakonda	University of North Carolina at Wilmington, USA
Omkar Dokur	University of South Florida, USA

Media Chair

Satish Maheshwaram	National Institute of Technology Warangal, India

Local Arrangement Chair

Prasanth Yanambaka	Texas Woman's University, USA

Special Session Chairs

Arslan Munir	Kansas State University, USA
Prasun Ghosal	IIEST Shibpur, India

Student Research Forum Chairs

Mike Borowczak	University of Wyoming, USA
Chenyun Pan	University of Texas at Arlington, USA

Research Demo Session Chairs

Amit Joshi	Malaviya National Institute of Technology Jaipur, India
Sibi Sethuraman	Vellore Institute of Technology AP, India

Finance Chair

Bibhudutta Rout	University of North Texas, USA

Registration Chair

Alakananda Mitra	University of Nebraska Lincoln, USA

Publicity Chairs

Umamaheswara Tida	North Dakota State University, USA
Uttam Ghosh	Meharry Medical College, USA
Hemanta Mondal	National Institute of Technology Durgapur, India
Sudeendra Kumar	PES University, India
Dhruva Ghai	Oriental University, India
Sujit Biswas	University of East London, UK
Theocharis Theocharides	University of Cyprus, Cyprus

Industry Liaison Chair

Robert Karam	University of South Florida, USA

Panel Chairs

Hao Zheng	University of South Florida, USA
Alex Chiumento	University of Twente, The Netherlands

Women in Engineering Chairs

Jaya Dofe	California State University, Fullerton, USA
Banee Bandana Das	SRM University AP, India

Steering Committee Chair

Srinivas Katkoori	University of South Florida, USA

Track Chairs

Regular Track - Artificial Intelligence and Machine Learning Technologies for IoT (AMT)

Sejun Song	University of Missouri Kansas City, USA
Yu Chen	Binghamton University, USA

Regular Track - Cyber Security/Privacy/Trust for IoT and CPS (SPT)

Filippo Malandra	University at Buffalo, USA
Kaustubh Dhondge	Glaukes Labs, USA

Regular Track - Electronics and Signal Processing for IoT (ESP)

Narayan Panigrahi	Center for AI and Robotics, India
Venkataramana Badarla	Indian Institute of Technology Tirupati, India

Regular Track - Hardware/Software Solutions for IoT and CPS (HSS)

Cihan Tunc	University of North Texas, USA
Tauhidur Rahman	Florida International University, USA

Regular Track - IoT or CPS Applications and Use Cases (APP)

Peeta Basa Pati	Amrita Vishwa Vidyapeetham, India
Pradip Sharma	University of Aberdeen, UK

Regular Track - Networking and Communications Technology for IoT (NCT)

Sergio Trilles	Universitat Jaume I, Spain
Xuyun Zhang	Macquarie University, Australia

Regular Track - Research Demo Session (RDS)

Amit Joshi	Malviya National Institute of Technology, India

Regular Track - Research Demo Session (RDS); Special Track - Metaverse for IoT (MIoT)

Sibi Chakkaravarthy Sethuraman	VIT-AP University, India

Regular Track - Student Research Forum (SRF)

Chenyun Pan	University of Texas at Arlington, USA
Mike Borowczak	University of Central Florida, USA

Regular Track - Women in Engineering (WIE)

Banee Das	SRM University Andhra Pradesh, India
Jaya Dofe	California State University Fullerton, USA

Special Track - AI and Big Data for Next-G Internet of Medical Things (IoMT)

Uttam Ghosh	Meharry Medical College, USA

Special Track - Blockchain for IoT-Driven Systems (BIoT)

Ashok Kumar Pradhan	SRM University Andhra Pradesh, India
Sujit Biswas	University of East London, UK

Special Track - Edge AI for Smart Wearables (EAW)

Bashir Morshed	Texas Tech University, USA

Special Track - Energy-Aware Security for IoT (EAS)

Sriram Sankaran	Amrita University, India
Swapnoneel Roy	University of North Florida, USA

Special Track - IoT for Smart Healthcare (SHC)

Abhishek Sharma	LNM Institute of Information Technology, India
Prateek Jain	Nirma University, India

Special Track - IoT for Wearables and Smart Devices (IWS)

Ramanujam E.	National Institute of Technology Silchar, India
Thinagaran Perumal	University Putra Malaysia, Malaysia

Special Track - Metaverse for IoT (MIoT)

Lei Chen	Georgia Southern University, USA
Meenalosini Cruz	Georgia Southern University, USA

Special Track - Security by Design for IoT (SbD)

Saswat Ram	SRM University Andhra Pradesh, India
Venkata Yanambaka	Texas Woman's University, USA

Special Track - Technologies for Smart Agriculture (TSA)

Alakananda Mitra	University of Nebraska Lincoln, USA
Laavanya Rachakonda	University of North Carolina Wilmington, USA

Technical Program Committee

Artificial Intelligence and Machine Learning Technologies for IoT (AMT)

Showmik Bhowmik	Jadavpur University, India
Jayson Boubin	Ohio State University, USA
Saptarshi Chatterjee	Jadavpur University, India
Te-Chuan Chiu	National Tsing Hua University, Taiwan
Uma Choppali	Dallas College - Eastfield Campus, USA

Soham Das	Microsoft, USA
Hongsheng Hu	Data61 CSIRO, Australia
Agbotiname Imoize	University of Lagos, Nigeria/Ruhr University Bochum, Germany
Hokeun Kim	Hanyang University, South Korea
Uma Maheswari B.	Amrita School of Engineering, India
Adnan Mahmood	Macquarie University, Australia
Pradip Pramanick	Tata Consultancy Services, India
Rajan Shankaran	Macquarie University, Australia
Sicong Shao	University of Arizona, USA
Yuan-Yao Shih	National Chung Cheng University, Taiwan
Ronghua Xu	Michigan Technological University, USA
Xiaonan Zhang	Florida State University, USA

IoT or CPS Applications and Use Cases (APP)

Showmik Bhowmik	Jadavpur University, India
Jayson Boubin	Ohio State University, USA
Saptarshi Chatterjee	Jadavpur University, India
Hongsheng Hu	Data61 CSIRO, Australia
Uma Maheswari B.	Amrita School of Engineering, India
Adnan Mahmood	Macquarie University, Australia
Pradip Pramanick	Tata Consultancy Services, India
Rajan Shankaran	Macquarie University, Australia
Praveen Shukla	Babu Banarasi Das University, India

Electronics and Signal Processing for IoT (ESP)

Showmik Bhowmik	Jadavpur University, India, India
Jayson Boubin	Ohio State University, USA
Saptarshi Chatterjee	Jadavpur University, India
Hongsheng Hu	Data61 CSIRO, Australia
Tanmay Kasbe	Shri Vaishnav Vidyapeeth Vishwavidyalaya Indore, India
Uma Maheswari B.	Amrita School of Engineering, India
Adnan Mahmood	Macquarie University, Australia
Tapas Patra	Odisha University of Technology and Research, India
Pradip Pramanick	Tata Consultancy Services, India
Md Abu Sayeed	Eastern New Mexico University, USA
Rajan Shankaran	Macquarie University, Australia
Vikas Tiwari	C.R. Rao AIMSCS, India

Hardware/Software Solutions for IoT and CPS (HSS)

Showmik Bhowmik	Jadavpur University, India
Jayson Boubin	Ohio State University, USA
Saptarshi Chatterjee	Jadavpur University, India
Uma Choppali	Dallas College - Eastfield Campus, USA

Garima Ghai	Oriental University Indore, India
Hongsheng Hu	Data61 CSIRO, Australia
Uma Maheswari B.	Amrita School of Engineering, India
Adnan Mahmood	Macquarie University, Australia
Ram Mohanty	UNSW Canberra, Australia
Pradip Pramanick	Tata Consultancy Services, India
Xiao Sha	Stony Brook University, USA
Rajan Shankaran	Macquarie University, Australia

Networking and Communications Technology for IoT (NCT)

Showmik Bhowmik	Jadavpur University, India
Jayson Boubin	Ohio State University, USA
Saptarshi Chatterjee	Jadavpur University, India
Joy Dutta	Khalifa University, United Arab Emirates
Umashankar Ghugar	GITAM University, India
Hongsheng Hu	Data61 CSIRO, Australia
Uma Maheswari B.	Amrita School of Engineering, India
Adnan Mahmood	Macquarie University, Australia
Pradip Pramanick	Tata Consultancy Services, India
Rajan Shankaran	Macquarie University, Australia

Contents – Part II

IoT or CPS Applications and Use Cases (APP)

Blockchain for IoT-Driven Systems (BIoT)

Networking and Communications Technology for IoT (NCT)

Security by Design for IoT (SbD)

IoT for Smart Healthcare (SHC)

Cyber Security/Privacy/Trust for IoT and CPS (SPT)

Research Demo Session (RDS)

Contents – Part I

Artificial Intelligence and Machine Learning Technologies for IoT (AMT)

Energy-Aware Security for IoT (EAS)

Edge AI for Smart Wearables (EAW)

Hardware/Software Solutions for IoT and CPS (HSS)

AI and Big Data for Next-G Internet of Medical Things (IoMT)

IoT for Wearables and Smart Devices (IWS)

Metaverse for IoT (MIoT)

Technologies for Smart Agriculture (TSA)

Student Research Forum (SRF)

IoT or CPS Applications and Use Cases (APP)

IoT Based Real Time Monitoring of Delhi-NCR Air Pollution Using Low Power Wide Area Network

Prem Chand Jain(✉), Vandavasi Satya Charan, Chitumalla Sahith, and Rohit Singh

Shiv Nadar University, Greater Noida, India
{Premchand.jain,vc885,cs172,rohit.singh}@snu.edu.in

Abstract. The clean and healthy air is essential for all living beings, and air pollution can have a significant impact on human health. It is important to monitor air quality in real time to take action to reduce the pollution level in order to maintain a healthy environment. As cities become more and more congested, the level of pollution is increasing, leading to a localized human health effects such as asthma or bronchitis. Implementation of Internet of Things (IoT) based technology with harmful gas sensors can be an effective solution for continuous monitoring of air quality. By using such a technology, one can gather data on harmful pollutants and take steps to minimize their impact on human health and the environment. In this paper IoT based continuous monitoring of the air pollution level of CO and CO_2 air pollutants carried out including temperature and humidity using different sensors and a micro-controller in Delhi-NCR (National Capital Region) at Greater Noida. The LoRa (**Lo**ng **Ra**nge) LPWAN (Low Power Wide Area Network) was used for data communication, and ThingSpeak an IoT analytics cloud service for storing and processing the data to be displayed on the web page. The LoRa is a wireless data communication technology, which is capable to transmit data to large distances using low power transmitter. The air quality monitoring was carried out by storing sensors data in the above cloud, analyzed, and compared with the standard air quality parameters.

Keywords: IoT · Air quality · Pollution · LoRa · LPWAN · Sensors

1 Introduction

Air is considered to be polluted when it contains certain substances in high concentrations and for long duration to cause harm or undesirable effects on human health. Air pollution is a significant concern in today's world, and it can have serious effects on human health. Fossil fuels (oil, gas, coal) are the main sources of air pollution. The fossil fuels is burnt to generate the electricity and automobiles that combust fuel. Reducing the use of fossil fuels and promoting renewable energy can help to reduce air pollution levels [1]. The air toxins are organic chemicals comprising molecules that contain carbon, hydrogen, and other atoms. The release of toxins by industries and emissions from the vehicles, as well

Published by Springer Nature Switzerland AG 2024
D. Puthal et al. (Eds.): IFIPIoT 2023, IFIP AICT 684, pp. 3–13, 2024.
https://doi.org/10.1007/978-3-031-45882-8_1

as natural sources such as wildfires and dust, all together contribute to the air pollution. As cities become more congested, the stationary sources such as factories, power plants, and smelters, while mobile sources such as cars, buses, trucks, and trains, all contribute to the air pollution. Therefore, it is necessary to take action to reduce air pollution to improve human health and the environment. Air pollution caused by CO, CO_2, SO_2, NO_2 and particulate matter such as PM2.5 and PM10 can have serious health impacts on individuals especially those who are already affected by respiratory conditions like asthma and chronic bronchitis. A mixture of particles with liquid droplets in the air forms Particulate Matter (PM). The PM2.5 represents by particles less than or equal to 2.5 μm in diameter while PM10 represents by particles less than or equal to 10 μm in diameter. The SO_2 is commonly found in industrial raw materials like coal, crude oil, and other resources. When they are burned during mining or industrial processes, they release sulfur gases due to incomplete combustion of the fossil fuels, which can cause respiratory diseases and irritation to the eyes. The CO is easily absorbed into the bloodstream, competing with the oxygen in hemoglobin, which can have serious health consequences. Higher concentration of CO_2 in the atmosphere deprived O_2 which can result in brain diseases [2]. Monitoring air quality is crucial in understanding the extent of pollution and the impact it has on people's health. In many developing countries, regulations have been introduced that require local authorities to conduct regular reviews of the air in urban areas where industrial activities and road transport produce high levels of pollutants. Accurate monitoring of pollutant concentration is essential in taking environment decisions and reducing pollution levels. To address the above issue, this paper discussed the design, development, and implementation of an IoT based wireless network using gas sensors to continuously monitor harmful pollutants using LoRaWAN technology. This approach provided an air quality data and helped to create awareness among the public about the harmful effects of air pollution. The air quality measurements and the reporting of the air pollution levels were carried out periodically. It helps to track the air pollution trends over time, identify the source of pollution, and to inform accordingly the decision about public health and environmental policy.

2 Delhi Air Pollution

There are several factors that contribute severe air pollution in Delhi [3]. Vehicular pollution is a major contributor to Delhi's air pollution. The city's growing population, increasing urbanization, and lack of efficient public transport systems have led to a rise in the number of vehicles on the road. Diesel vehicles, in particular, emit higher level of particulate matter and nitrogen oxides, which are major contributors to the air pollution. Delhi is surrounded by several industrial areas like Noida, Ghaziabad, Faridabad which are a significant source of air pollution. The industries located in above areas emit a range of pollutants, including sulfur dioxide, nitrogen oxides, and particulate matter. During the winter months, farmers in the neighboring states of Punjab and Haryana burn crop residues to clear their fields for the next crop. This practice known as stubble burning, releases a large amount of particulate matter and other pollutants into the air, which contributes to the severe air pollution in Delhi. Garbage burning is another significant contributor to Delhi's air pollution. In many areas, people dispose of their waste by burning it, which releases harmful pollutants into the air. Construction work is going on for big projects in Delhi-NCR which is a major contributor to the dust pollution in those construction sites. During the winter months, Delhi experiences a phenomenon known as a “temperature inversion”, which traps pollutants close to the ground, leading to high levels of pollution. The Fog is a form of cloud on the earth’s surface containing tiny water droplets. The Smog is an intense form of air pollution which is a mixture of fog, smoke, and particulate matter. The Delhi location is in a semi-arid region with little rainfall, and hence high level of dust exacerbate the problem. The smoke which would otherwise have been hanging higher in the sky while the dust particles which would have landed on the ground, they remain suspended in the air and as they mix with fog, generate smog. The landlocked geography of Delhi causes air pollution. The North-Westerly winds coming from Rajasthan brings dust to the region while Himalayas obstruct the escape route of the air. This causes the dust and pollutants to settle in the region. Overall, Delhi’s air pollution is a complex issue that requires a multi-faceted solution, including better public transportation, strict emission standards for vehicles and industries, improved waste management practices, and policies to address agricultural burnings.

3 Low Power Wide Area Network

Designers of IoT sensor and actuator networks for air quality monitoring requires long range wireless communication that is secure, robust, low maintenance, and relatively easy to deploy. The LPWAN (Low Power Wide Area Network) includes LoRaWAN and Sigfox technology using unlicensed frequency spectrum, while the cellular 4G-LTE (Long Term Evolution)-M (Machine) and Narrow band (NB)-IoT with licensed frequency spectrum permits end nodes to move seamlessly throughout the wireless network without interruption of the network. NB-IoT promises for LPWAN applications while LTE-M promises for mission critical or more data intensive applications. In this paper LoRa technology was used, which enabled long-range communication and provided robustness against interference. The LoRaWAN is an open protocol based on LoRa technology, which is a robust and mature protocol that enables long-range, low power, wireless communication for IoT sensor and actuator networks [4]. The LoRaWAN protocol defined the system architecture for the network is shown in Fig. 1 which has a significant influence on the battery life, network capacity, quality of service, and security. The LoRaWAN uses a narrow band modulation scheme at sub-GHz frequencies, and it uses a modified form of Direct Sequence Spread Spectrum (DSSS) called Chirp Spread Spectrum (CSS) to spread the narrow band signal over a wider bandwidth. The DSSS requires highly accurate clock sync. While the CSS modified version of DSSS eliminates the clock sync. issue in LoRa. The CSS spreads the narrow band signal by generating a chirp signal that continuously varies in the frequency. In LoRaWAN network the end IoT nodes are sensors/actuators built with micro-controller and LoRaWAN transceiver. The end nodes gathers sensor data and transmits to one or more LoRa gateways. They are remotely connected and are battery operated. The LoRaWAN protocol operates in a star topology, where the end nodes connect directly with the gateway, and the gateway acts as a bridge between the end nodes and the network server. The end nodes data received by the gateways are forwarded to the cloud-based network server via some back-haul using cellular, satellite, or WiFi communication as shown in Fig. 1. The network server gathers data from multiple gateways, filters duplicate messages, decides which gateway should respond to the end node message, and adapt data rates to extend the battery life of the end nodes. The network server handles all the intelligence and complexity associated for managing the network. The application server collects information from network server and controls the actions of the end nodes. The LoRaWAN provides different classes of operation that allow a trade-off between power consumption and latency. Class A provides bidirectional communication with lowest transmit power but the largest latency. The end nodes transmit data to the gateway only when they have data and become inactive until the next data transmission. Class C provides continuous listening and down link the data reception at any time providing the lowest latency, but the end node receiver is always on. Class B provides moderate power consumption and moderate latency. The LoRaWAN is relatively easy to deploy communication protocols and system architecture for the IoT sensor and actuator networks for the air quality monitoring, making it an excellent choice for this application.

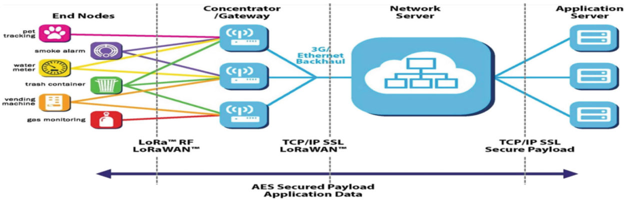


Fig. 1. LoRaWAN Architecture: Ref. [4]

4 Related Work

Reference [5] monitored air quality by taking data from the web servers. Provision was made to trigger alarm when the air quality goes down beyond a certain level and also displayed on the LCD display the web page along with preventive measures. Pollution could be monitored from anywhere using mobile phone interface. Reference [6] measured real time air quality using PMS5003T sensors and several LoRa nodes. Data analyzed using ThingSpeak cloud. Reference [7] designed smart gas meter using LoRa RFM95 hardware. The data was sent to Antares Cloud. The LoRaWAN protocol was used to communicate data between LoRa RFM95 hardware and Antares Cloud. Reference [8] monitored air quality using Raspberry Pi4 platform. The Code was written in Python, and MQTT protocol used as broker. Data was uploaded on ThingSpeak cloud to analyze. Reference [9] monitored carbon dioxide level using LoRaWAN. User could access data from web server. Reference [10] monitored temperature, humidity, pressure, and smoke using respective sensors on nodeMCU platform which had inbuilt WiFi module. MQTT client transferred the data to ThingSpeak cloud which displayed on the web page. Reference [11] used mobile air pollution monitoring stations by mounting sensors on existing public vehicles to gather spatio-temporal air pollution data. With this a few mobile stations could map the entire city at high resolution in place of mounting a large number of fixed air pollution monitoring stations in the entire city which will be quite costly compared to a few mobile air pollution stations.

5 Methodology

5.1 System Hardware Design

The system architecture shown in Fig. 2 was designed using ATmega328P-AU micro-controller (Arduino Uno board) that is connected to different sensors to measure the parameters such as temperature, humidity, gas content of CO and CO_2. The micro-controller process the sensor data, and sends the data using LoRaWAN communication module SX1276 LoRa Shield to LG01N LoRa Gateway. The ATmega328P-AU is a low-power 8-bit CMOS micro-controller that improves AVR (Advanced Virtual RISC) by running strong tracking in a single clock cycle. It works at 1 MIPS per MHz. The SX1276 is a low power long range transceiver module which uses chirp spread spectrum modulation to overcome interference in the medium. The LG01N single channel LoRa Gateway bridges between the LoRa SX1276 and a ThingSpeak cloud. The data from gateway to cloud is transmitted through backhaul using WiFi, 4G, 5G cellular, or Ethernet. The data received in the cloud is further processed and displayed on a web application. The LG01N gateway runs on an open source embedded Linux system. It has a micro-controller (ATMega328P) which connects the LoRa module (SX1276) with the linux module (ar9331 processor) which has WiFi capabilities. The DHT11 sensor is used to measure the temperature and humidity of the air. It sends data in digital format. It can measure the temperature from 0 °C to 50 °C and Humidity from 20% to 90%. The MQ-135 sensor is used to measure the levels of harmful gases in the air. It detects gases like Ammonia (NH_3), sulfur dioxide (SO_2), Benzene (C_6H_6), Carbon Dioxide (CO_2), and other harmful gases but MQ-135 Sensor is most sensitive to Carbon Dioxide. The values which are measured from the MQ135 Sensor gives the approximate value of AQI (Air Quality Index). The MQ-7 sensor is used to measure Carbon Monoxide. It contains a sensing element of aluminum-oxide, which is a ceramic coated with Tin dioxide (SnO_2), and enclosed in a stainless- steel mesh.

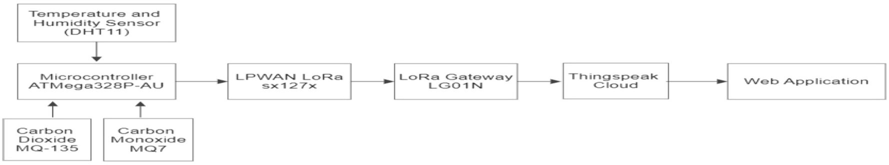


Fig. 2. System Block Diagram

5.2 MQTT Protocol

MQTT (Message Queuing Telemetry Transport) is a connectivity protocol of Internet of Things. It is a simple messaging protocol which can be used for constrained devices with low bandwidth. In this paper MQTT protocol is used to publish the data received from the sensor nodes to the ThingSpeak cloud through the LG01N Gateway. The ThingSpeak has a MQTT broker URL "mqtt3.thingspeak.com." Data can be published to the cloud using topic format "channels/channelID/publish", and payload format "field1 = x and field2 = y". The LG01N gateway has an inbuilt configuration for the MQTT protocol. All the required MQTT settings can be applied to the web interface of the gateway. It has a built-in Linux utility mosquito that can be used to publish the data to ThingSpeak. It receives LoRa packets from an end node and forwards them to ThingSpeak via MQTT over the Internet.

5.3 Air Quality Index

Air Quality Index (AQI) is an index which is used for measuring the air quality [12]. AQI is measured on a scale of 0–500. The air is more dangerous when the AQI is higher and good when it is lower. The lower the AQI, the better for the human beings. There are some major pollutants like carbon monoxide (CO), carbon dioxide (CO_2), nitrogen dioxide (NO_2), sulfur dioxide (SO_2), ammonia (NH_3), lead (Pb), PM2.5, PM10, which are considered for calculating the AQI. Although Carbon dioxide (CO_2) is not a pollutant in the air, but Oxygen deprivation could occur if the value goes above 2000 ppm. The concentration of each of the major pollutant is considered and a sub-index is calculated for each component based upon the standard parameters. The worst of the sub-index is considered as an Air Quality Index. The Table 1 shows the standard values for AQI, CO, and $CO_{2.}$ As an example, the AQI in Delhi was 408 in Anand Vihar, 447 in Bawana, 404 in Patpargang, and 411 in Wazirpur on 30 Oct., 2021:9.25 IST [*Ref*.:India Today Web Desk].

Table 1. Air Quality Index and CO and CO_2 Standard Parameters

Category	AQI	CO (ppm)	CO_2 (ppm)
Good	0–50	0.0–4.4	400–700
Satisfactory	51–100	4.5–9.4	701–1000
Moderate	101–200	9.5–15.4	-
Poor	201–300	15.5–30.4	101–1500
Very Poor	301–400	30.5–40.4	1501–2000
Severe	401–500	40.5–50.4	2001–5000

6 System Implementation

6.1 Hardware Implementation

Hardware included Dragino SX1276 LoRa shield with an Arduino Uno micro-controller board, LG01-N LoRa Gateway, and various sensors DHT11, MQ135, and MQ7 to measure the air quality. The hardware shown in Fig. 3 included sensors connected to the Arduino board with LoRa shield shown at top left in the figure. The Arduino IDE was used to download the required sensor libraries of DHT11, MQ135 and MQ7. Measurements of temperature and humidity were carried out using DHT11 sensor shown at bottom left in the figure, AQI and Carbon dioxide using MQ135 sensor shown at bottom middle, and Carbon monoxide using MQ7 sensor shown at bottom right in the figure. All these sensors were connected to the breadboard (bottom), and analog/digital connections were made to the Arduino Uno micro-controller as shown in Fig. 3. A total of 6 functions were defined out of which 4 functions were used to read the required values from the sensors, and assigned them the variables and other functions to write the data into a single string of required format to transmit the data packets. The single stream sample shown in Fig. 4 displayed as field1 = 25 Temperature, field2 = 54 Humidity, field3 = 423 AQI, field4 = 8.8 CO, and field5 = 418.4 CO_2 at third line from bottom.

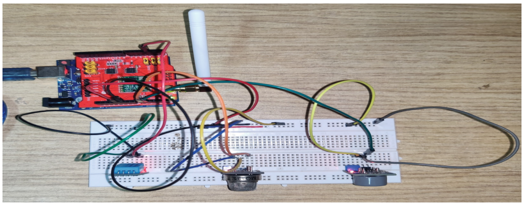
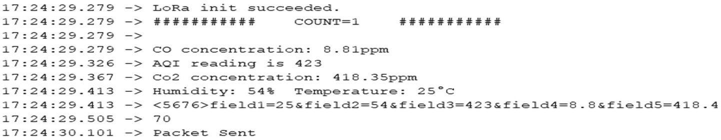


Fig. 3. DHT11, MQ135, MQ7 Sensor Connected to the Arduino + LoRa Board



```
17:24:29.279 -> LoRa init succeeded.
17:24:29.279 -> ###########    COUNT=1    ###########
17:24:29.279 ->
17:24:29.279 -> CO concentration: 8.81ppm
17:24:29.326 -> AQI reading is 423
17:24:29.367 -> Co2 concentration: 418.35ppm
17:24:29.413 -> Humidity: 54%  Temperature: 25°C
17:24:29.413 -> <5676>field1=25&field2=54&field3=423&field4=8.8&field5=418.4
17:24:29.505 -> 70
17:24:30.101 -> Packet Sent
```

Fig. 4. Display of Transmitted Packet Details

Lora library was installed for transmitting the data. All the required parameters, such as node ID (local Channel ID), frequency, coding rate, bandwidth, etc., were specified to match the gateway parameters. While sending the data, the node ID value was specified which was used during the setup of MQTT in the gateway. This node ID helped the gateway to recognize the LoRa node and publish the data that has been received by the respective channel using MQTT.

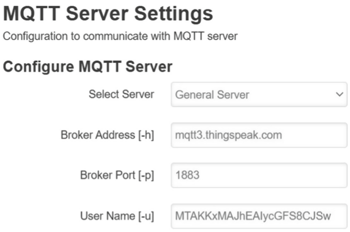
6.2 LoRa Gateway Interface

LoRa Gateway received data from number of LoRa end nodes. It was configured using a laptop by connecting it to the network through LAN cable. It had a default IP address of 10.130.1.1. Clicking on it, will open a login interface with a default username and password. After login, a complete interface for modifying the settings was displayed. The gateway needed to be connected to a WiFi network for connecting the Internet, which was done using network scanning. The gateway was connected to the mobile hotspot, and the default WiFi access point (AP) named dragino-1d143c was disabled, which showed that the gateway was successfully connected to the Internet [13].

In the web interface of the gateway, the LoRaWAN server settings were changed to LoRARAW forwarded to MQTT. This enabled MQTT connection through the gateway. In MQTT settings, the required parameters like username, password, clientID, broker address, port, topic format, and data format were set as shown in Fig. 5. A new channel was created with the local Channel ID (LoRa node) and Remote Channel ID (ThingSpeak). The gateway used these IDs to detect the incoming message from the LoRa end node and published it to the right channel in ThingSpeak.

6.3 ThingSpeak Cloud Server Settings

A new channel was created using five fields for temperature, humidity, AQI, CO, CO_2 to store the data sent by the gateway. A new MQTT device was set up which was done by selecting the devices option in the navigation bar (Fig. 6). A temperature sensor device was setup which gave the MQTT clientID, and was used for setting up a connection from the gateway. Access was given to the required channel to publish the data from the gateway.



MQTT Server Settings

Configuration to communicate with MQTT server

Configure MQTT Server

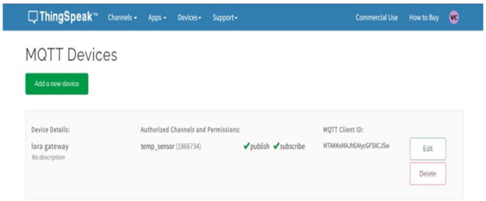
Select Server: General Server

Broker Address [-h]: mqtt3.thingspeak.com

Broker Port [-p]: 1883

User Name [-u]: MTAKKxMAJhEAlycGFS8CJSw

Fig. 5. Gateway MQTT settings



MQTT Devices

Device Details: lora gateway, No description

Authorized Channels and Permissions: temp_sensor (1866734) ✓publish ✓subscribe

MQTT Client ID: MTAKKxMAJhEAlycGFS8CJSw

Fig. 6. ThingSpeak MQTT settings

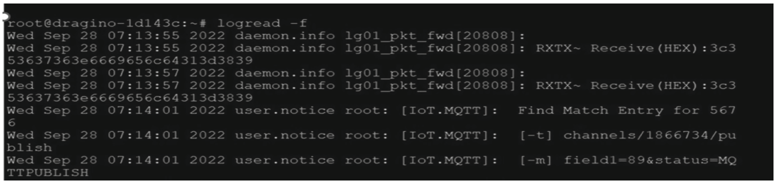
6.4 User Interface Settings

A website was created which was used to display the measured values of the sensors. This website was made using React.js which is a front-end javascript library. Different components like the navigation bar, boxes to display data, graphs showing previous results were designed. The data displayed in the website was updated live from the values fetched from the thingspeak cloud without needing a page refresh. The data was fetched from ThingSpeak using REST API calls. Using axios function in react, GET request was made to the ThingSpeak API endpoint. The function returned all the required data. This data was processed and all the required data was obtained from the response. The data was fetched continuously and updated in the website. The graphs in ThingSpeak provided visualization of the data collected. This can be used to look at previous data and analyze the data. The HTML iframes were used to display the graphs in the website. The iframes were embedded in the website code and were updated live.

7 Results

7.1 Data Flow from LoRa End Node to the Website Testing

The code was finalized and uploaded to the board. The data from all the sensors were collected, and LoRa packets were transmitted by the LoRa end node. Gateway's Linux SSH was accessed using the putty tool. Logread command was used to read the logs of the gateway. The packet received from the node can be seen in the logs, and it was published to the set MQTT channel as desired (Fig. 7). The data sent from the LoRa end node was successfully uploaded to the ThingSpeak cloud using MQTT. The data from ThingSpeak was continuously updated in the website without refreshing the page.



```
root@dragino-1d143c:~# logread -f
Wed Sep 28 07:13:55 2022 daemon.info lg01_pkt_fwd[20808]:
Wed Sep 28 07:13:55 2022 daemon.info lg01_pkt_fwd[20808]: RXTX~ Receive(HEX):3c3
53637363e6669656c64313d3839
Wed Sep 28 07:13:57 2022 daemon.info lg01_pkt_fwd[20808]:
Wed Sep 28 07:13:57 2022 daemon.info lg01_pkt_fwd[20808]: RXTX~ Receive(HEX):3c3
53637363e6669656c64313d3839
Wed Sep 28 07:14:01 2022 user.notice root: [IoT.MQTT]:  Find Match Entry for 567
6
Wed Sep 28 07:14:01 2022 user.notice root: [IoT.MQTT]:  [-t] channels/1866734/pu
blish
Wed Sep 28 07:14:01 2022 user.notice root: [IoT.MQTT]:  [-m] field1=89&status=MQ
TTPUBLISH
```

Fig. 7. Gateway Showing Received Packets and MQTT Publish

7.2 Outdoor Testing Results

Air quality was monitored outside the lab at Shiv Nadar University, G. Noida by taking the LoRa node to different places. The 300 m range was chosen because of WiFi used as a backhaul with obstacles. The gateway was placed inside hostel Dibang and measurements were carried out. The measurements were taken periodically every 10 min. The measurements at the Dibang hostel opposite lawns at 7.10PM showed the AQI with poor category (275), however, CO_2 concentration was good (412 ppm) and CO concentration was satisfactory (7.2 ppm) as shown in Fig. 8. The measurements at the Inner Gate at 12.20PM showed the AQI in very poor category (364), however, CO_2 concentration was good (443 ppm) and CO concentration was satisfactory (8.1 ppm) as shown in Fig. 9. The measurements at the Mini Mart at 2.10PM showed the AQI again in very poor category (342), however, CO_2 concentration was good (464 ppm), and CO concentration was satisfactory (8.7 ppm) as shown in Fig. 10.

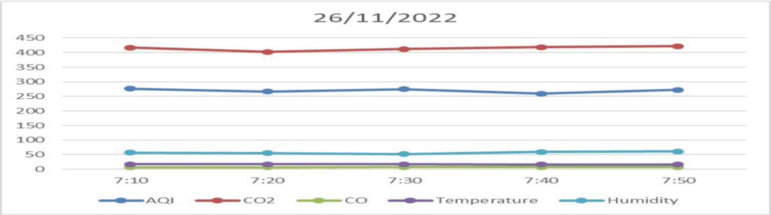


Fig. 8. Measurements taken from Hostel Dibang opposite lawn at 7PM on 26/11/2022

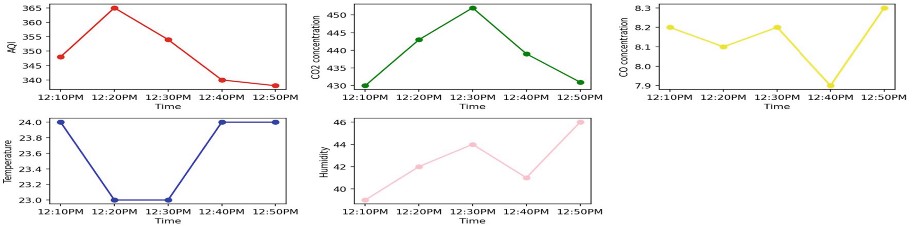


Fig. 9. Measurements taken from Inner Gate at 12Noon on 27/11/2022

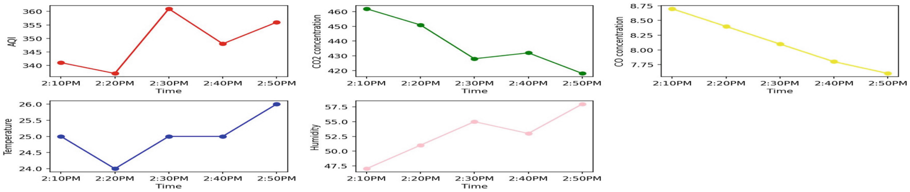


Fig. 10. Measurements taken from Mini Mart at 2PM on 28/11/2022

8 Conclusions

The IoT based air pollution monitoring system using LoRa LPWAN was designed and implemented. Measurements of temperature, humidity, carbon monoxide and carbon dioxide concentration, and Air Quality Index were carried out. LoRa data packets were transmitted and uploaded to the cloud using the gateway, and displayed on a web page in the form of graphs. Air quality was tested in three different places in the Shiv Nadar University, G. Noida. It can be tested other nearby places like Noida, Dadri, Faridabad, Delhi, etc. where pollution is quite significant. This system can be used to monitor the air quality data to take the necessary precautions and also helps to create awareness about the air quality around us. In future, other pollutants like NH_3, NO_2, SO_2, PM2.5, PM10 which affect the air quality can be introduced. Alarming system can also be introduced to alert the user through SMS or email. User can interface with website and take necessary action to purify the air environment by actuating smoke purifiers. The air pollution data can be integrated into a smart city system for monitoring and controlling the air quality and pollution level in the city. It can help the city authorities to take necessary action in case of high pollution levels. The air pollution is dynamic with locations and time. It exhibit different air pollution levels a few hundred meters away and also vary at different times of the day. To handle such a situation, a large number of fixed air pollution monitoring stations are required in the entire city which will be quite costly. However, the mobile air pollution monitoring stations built by mounting sensors on the existing public vehicles can be used to tackle this issue. A combination of fixed and mobile air pollution monitoring stations network can provide maximum coverage and temporal resolution. Machine Learning (ML) concept can be introduced for making predictions of air quality. The data collected and stored for long time can be applied as an input to ML algorithm to predict the air quality to take the preventive action beforehand.

Acknowledgments. The authors are thankful to Prof. Dinkar Prasad, Head, EE Dept., and Associate Dean, School of Engineering, for providing necessary resources and infrastructure to complete this project, and to Prof. S. Sen, Dean, School of Engg., Shiv Nadar University, G. Noida (UP) for his encouragement, and permission to publish this paper.

References

1. The sources and solution: Fossil Fuels. US-Environmental Protection Agency (2023)
2. Nathanson, J.A.:Air pollution control. In: Encyclopedia Britannica (2023)
3. Air pollution in Delhi-Wikipedia. http://en.wikipedia.org/wiki/Air_pollution-in-Delhi
4. Raja, U., Kulkarni, P., Sooriyabandara, M.: LPWAN: an overview. IEEE Commun. Surv. Tut. **19**, 855–873 (2017)
5. Poonam, P., Ritik, G., Sanjana, T., Ashutosh, S.: IoT based air pollution monitoring system. Int. Res. J. Eng. Technol. IRJET **4**, 1137–1140 (2017)
6. Od, S., Huang, H.H., Wei, J.B.: Apply LoRa technology to construct an air quality monitoring IoT system. In 2021 IEEE 3rd Eurasia Conference on Biomedical Engineering, Healthcare and Sustainability (ECBIOS), pp. 88–91 (2021)
7. Prabowo, M.C.A., Hidayat, S.S., Luthfi, F.: Low cost wireless sensor network for smart gas metering using antar iot platform. In: 2020 International Conference on Applied Science and Technology (ICAST), pp. 175–180 (2020)
8. Faiazuddin, S., Lakshmaiah, M., Alam, K.T., Ravikiran, M.: IoT based indoor air quality monitoring system using Raspberry Pi4. In: Proceedings of the 4th International Conference on Electronics, Communication and Aerospace Technology (ICECA) (2020)
9. Twahirwa, E., Mtonga, K., Ngabo, D., Kumaran, S.: A LoRa enabled IoT-based air quality monitoring system for smart city. In: 2021 IEEE World AI IoT Congress (AIIoT), pp. 0379–0385(2021)
10. Kumari, N., Sakshi, Gosavi, S., Nagre, S.S.: Real-time cloud based weather monitoring system. In: 2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), pp. 25–29 (2020)
11. Swaminathan, S., et al.: Data science and IoT based mobile monitoring framework for hyper-local PM2.5 assessment in urban setting. Build. Environ. **225**, 109597 (2022). https://doi.org/10.1016/j.buildenv.2022.109597
12. New Delhi Air Quality index (AQI): Real time air pollution. http://www.aqi.in/dasfboard/india/delhi/new-delhi
13. Dragino: Dragino single channel LoRa IoT kit user manual. [Online]. https://www.dragino.com/downloads/downloads/LoRaIoTKit/v2-Kit/Single%20Channel%20LoRa%20IoT%20Kit%20v2%20User%20Manualv1.0.7.pdf

A Survey of Pedestrian to Infrastructure Communication System for Pedestrian Safety: System Components and Design Challenges

Pallavi Zambare(✉) and Ying Liu(✉)

Texas Tech University, Lubbock, USA
{pzambare,Y.Liu}@ttu.edu

Abstract. As urbanization continues to grow and smart cities are imagined, intelligent transportation systems (ITS) have become increasingly important as a solution to traffic congestion. While ITS focuses on vehicles, pedestrians are important road users who contribute a significant role in influencing traffic, transportation infrastructure, and the design of vehicles, However, roadside assistance is less studied than vehicular. In this paper, we discuss pedestrian-to-infrastructure (P2I) communication, which is an important aspect of ITS that can enhance safety, efficiency, and convenience for pedestrians. Furthermore, P2I systems are examined in terms of their requirements and components, as well as in terms of their potential benefits for safety and mobility issues. Finally, the paper identifies potential future directions for research on pedestrian-to-infrastructure communication in ITS. Providing a comprehensive overview of the current state of research on pedestrian-to-infrastructure communication in ITS, this review highlights the key research areas for the future.

Keywords: Intelligent Transportation system (ITS) · Pedestrian safety · Pedestrian-to-infrastructure communication (P2I) · Internet of Things · Pedestrian-to-everything (P2X)

1 Introduction

Pedestrian safety has always been a top priority in transportation systems. However, the rapid development of cities has led to a significant increase in threats to non-motorists and motorists alike, including pedestrians, bicyclists, vehicle accidents, and air pollution, due to this pedestrians and vehicular travelers waste a lot of time while traveling. According to [1,2] recent report by the government, pedestrians in congested traffic areas are facing a serious threat of injury from traffic accidents. The report concludes that the current traffic management system should be re-designed and re-evaluated to address safety issues efficiently, especially for vulnerable road users (VRUs).

Published by Springer Nature Switzerland AG 2024
D. Puthal et al. (Eds.): IFIPIoT 2023, IFIP AICT 684, pp. 14–35, 2024.
https://doi.org/10.1007/978-3-031-45882-8_2

To address frequently occurring non-motorist accidents, several innovative approaches have emerged, including those designed to mitigate intersection collisions involving VRUs [3]. Moreover, various types of sensors have been developed to detect safety issues related to VRUs. These sensors include activated sensors mounted on vehicles or along roads, as well as radars, cameras, Lidars (Laser Imaging Detection and Ranging), and IMUs (inertial measurement units) integrated into smartphones. Based on the capabilities and characteristics of these sensors, several systems have been developed to protect VRUs [4]. For instance, perception-based systems with a limited field of view (FOV) can detect and alert drivers to VRUs within their range. These systems work in tandem with other technologies such as vehicle-to-pedestrian (V2P) communication and vehicle-to-everything (V2X) systems, to enhance safety for VRUs [5].

Ensuring pedestrian safety is a multifaceted challenge that requires attention not only to the end system but also to the communication and inference capabilities that underpin traffic efficiency and mobility. To meet the demands of modern transportation systems, these capabilities must be re-examined and adapted accordingly. In this context, it is critical to adopt an all-encompassing approach to protecting pedestrians within communication systems. To minimize latency for safety-critical alerts and enable real-time communication, pedestrians should be able to communicate using a range of channels that reduce message congestion and bandwidth usage. This is where pedestrian-to-everything (P2X) comes into play, encompassing pedestrian-to-pedestrian (P2P), pedestrian-to-vehicle (P2V), and pedestrian-to-infrastructure (P2I), communication channels that facilitate seamless sharing of traffic data. The P2I communication system plays a crucial role in facilitating data communication from pedestrian to infrastructure for inference and applications. However, its development has been slower compared to P2V communication, mainly due to high costs and the difficulty of upgrades. Fortunately, with the advent of software-defined ITS, there are opportunities to improve the overall architecture and facilitate the application of new inference algorithms in a more flexible manner.

To provide a comprehensive overview of the P2I communication system, this survey also describes P2I's various system components and their functions. Additionally, this survey highlights our contribution in this field and summarizes the corresponding sections as follows: In Sect. 2, we discuss pedestrian-to-infrastructure system architectural components. Section 3 focuses on pedestrian-infrastructure communication. Section 4 We discuss P2I communication systems that must meet a set of requirements. Section 5 highlights design challenges of P2I System. Finally, the paper concludes in Sect. 6.

2 Pedestrian to Infrastructure System Architecture

A pedestrian-to-infrastructure (P2I) system involves using technology as a means of facilitating interaction and communication between pedestrians and the surrounding built environment, which consists of buildings, roadways, and public transportation systems. The architecture of P2I systems are typically composed of several components that work together to achieve specific goals, such as improving pedestrian safety, accessibility, and convenience.

The P2I communications support a broad range of applications that support both pedestrian convenience and pedestrian safety. Safety applications include collision detection, collision avoidance, and other safety applications that can improve pedestrian efficiency and safety. In addition to retrieving data from VRUs to better understand the overall Real-time traffic information, convenience applications can also include Safety alerts, Personalized recommendations, and public transportation integration. P2I communication systems can be used with this type of application, but more investment is needed in the field of digital infrastructure to take advantage of it. In addition, the P2I system operates in three stages: detection of pedestrians, tracking of pedestrians, and prediction of pedestrian trajectory followed by action [5,6]. As a result of these elements, different P2I system architectures have been developed. This section provides a brief overview of the various P2I architectural components.

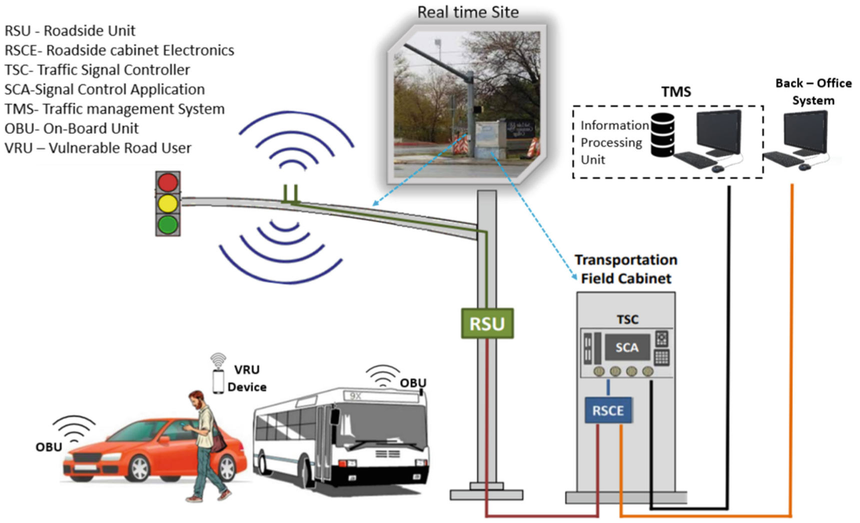

RSU - Roadside Unit
RSCE- Roadside cabinet Electronics
TSC- Traffic Signal Controller
SCA-Signal Control Application
TMS- Traffic management System
OBU- On-Board Unit
VRU – Vulnerable Road User
Real time Site
TMS
Back – Office System
Information Processing Unit
Transportation Field Cabinet
TSC
SCA
RSCE
RSU
VRU Device
OBU
OBU

Fig. 1. Components of P2I functional architecture

2.1 Components of a Pedestrian to Infrastructure System

The exchange of critical information using P2X communications can improve road safety and mobility for vulnerable road users and other road users. By receiving real-time information about infrastructure (e.g., traffic signal timings and phases, intersection geometry), road users can travel more efficiently, reduce delays, and reduce emissions. To reduce congestion and improve mobility, operators in traffic management centers (TMCs) can implement active or proactive traffic management strategies after receiving real-time information from OBUs or VRUs. Figure 1: describes the components of digital infrastructure. Connected vehicles (CV) usually have an onboard unit (OBU) and pedestrians usually have a Vulnerable Road User device (VRU) which allows them to wirelessly communicate and share information with roadside units (RSUs). The RSU is an important element of the system since it exchanges data with the OBUs and VRUs, as well as other infrastructure components. Communication units are located on RSUs along roads such as traffic cameras or traffic signals, which establish communication links with vehicles based nearby. RSUs can communicate via Wi-Fi, WiMAX, ZigBee, Bluetooth, and cellular networks, among others RSUs can receive messages from OBUs or VRU devices and forward these messages to transportation infrastructure elements via the transportation field cabinet (e.g., traffic management systems, traffic signal controllers (TSCs), and back-office data storage) to provide information about real-time traffic conditions.

The components of P2I systems can be generally divided into the following categories:

1. Devices for pedestrians or VRU devices (Smartphone, Wearable sensors)
2. Vehicle-mounted devices (On-board devices)
3. Infrastructure (RSU)
4. Information processing unit

Whenever a P2I system depends entirely on direct communication, it consists of only two components. The infrastructure and the pedestrian device. All three phases of the P2I system are carried out by these two components. In the case of a system where indirect communication is used (i.e., through infrastructure), the tracking, detection, and trajectory prediction phases are handled by an information processing unit. The probability of a crash is estimated based on pedestrian trajectory prediction. As a result, the infrastructure notifies the Vehicle and VRU devices to take the necessary action, as needed. Therefore, the VRU device and vehicle device may take appropriate action.

1. **Devices for pedestrians or VRU devices (Smartphone, Wearable sensors)**
   - **Smart phone:** Mobile phones may prove to be the most widely accepted VRU device due to their ubiquitous and adaptable nature. Smartphones have been used as VRU devices in P2I communication. Currently, available commercial off-the-shelf (COTS) smartphones are equipped with sensors like accelerometers, GPS, Bluetooth, Wi-Fi, communication technologies like cellular (LTE/3G) etc. In order to develop effective P2I systems, sensors and communication technologies must be integrated. In addition to audio-visual and haptic warnings, smartphones can also provide these functions. A P2I system that incorporates VRU warnings may find this useful [7].
   - **Helmet:** Cycling helmets and motorcycle helmets can be used as VRU devices. It is, however, necessary for the helmet to be equipped with the essential components to serve as a VRU. The helmet and smartphone

used by Hernandez-Jayo et al. [8] serve as a VRU device for cyclists. This system transmits position data from the smartphone to the cloud. Helmets are used to alert cyclists to vehicles in their path.

- **Tag:** P2I systems may use tags as VRU devices where unilateral warnings (to the driver only) are sufficient. Tags can be attached to backpacks, wheelchairs, handbags, etc. [9]. These tags can be used as VRU devices. It is possible for the tag to not engage in active P2I communication and to only reply when a vehicle device is detected.
- **Smart watches:** P2I communication systems are able to monitor pedestrian traffic with smartwatches as VRU devices. In order to improve pedestrian safety and optimize traffic flow, traffic engineers can collect data from smartwatches worn by pedestrians. The use of smartwatches in P2I communication systems enhances pedestrian safety by providing pedestrians with real-time information about traffic. Pedestrians can also get haptic feedback from smartwatches, such as vibrations, to be alerted to approaching vehicles [10].

2. **Vehicle-mounted devices (On-board devices)**
A vehicle's OBU transmits and collects data for a variety of purposes. The OBU (on-board unit) is an electronic device incorporated into a vehicle that monitors traffic and driving records and can be connected to roadside systems and satellite navigation systems. In general, they are used to automate toll collection and billing, referred to as electronic toll collection (ETC), but they can also provide additional services. An OBU can be used to store diagnostic and emergency data, plan routes, and navigate. Further, they are capable of communicating with vehicles-to-vehicles, vehicles-to-infrastructures, and vehicles-to-roadsides. OBUs are typically used in tolls to communicate with the tolling system and determine the distance traveled and the amount of toll to pay. Radio and mobile radio technology as well as satellite navigation are the two most common methods used. A radio beacon transmits a signal that is received by the OBU using radio technology. OBUs modulate that signal and send back data to beacons. It is possible to determine the distance traveled by the beacon based on its stationary position. OBUs are equipped with GPS receivers when using satellite navigation for tolling. OBUs send data via SMS to toll centers via GSM modems. This navigation data is then used to calculate the toll, which may also include other vehicle-specific information, such as the exhaust gas class and axle count. A driver can use OBUs to receive ITS services including warnings and travel information when they are used for emergency data. Using Basic Safety Messages (BSMs), OBUs continually communicate with other vehicles, roadside units (RSUs), and other devices [11].
3. **Infrastructure (RSU)**
A RSU entity can be considered one of the essential components of an ITS system. This can be implemented in the form of a base station or a dedicated stationary entity installed along the road. This device is equipped with a DSRC interface, which enables communication with any component with the same interface (vehicle, RSU, etc.). The communication range can

vary depending on the technology and environment. As an example, an RSU entity that supports the DSRC standard has a communication range of 300 m in urban environments, and a range of up to 1 km in rural settings. A Roadside Unit may be wired or wirelessly interconnected, and it can provide not only local services but also cloud services and/or Internet access to different vehicles by using RSU, roads can communicate with their users, such as pedestrians and vehicles, through Infrastructure to Infrastructure (I2I), Vehicle to Infrastructure (V2I), and Pedestrian to Infrastructure (P2I). In order to resolve road issues, as well as pedestrian safety issues, a variety of communication has been developed for road infrastructure. Using I2I communication, traffic conditions of various road segments can be exchanged. This can help traffic lights, for instance, customize light phases based on global road conditions. By combining I2I with P2I, I2I can alert pedestrians (in addition to other RUs) about emerging incidents on their way. As a result, the pedestrian can choose a safer route. In addition to virtual traffic lights, virtual traffic lights can also be used to manage crossings for pedestrian safety. Essentially, VTL is an infrastructure-free traffic control method that utilizes vehicle-to-vehicle (V2V) communication and uses this information to determine the individual traffic signal for all vehicles, using a lead car that rotates every cycle, and determining the individual traffic signal for every vehicle in the area [12]. A VTL system has been proposed recently for vehicular traffic management at intersections, but its ability to accommodate pedestrian crossing policies has not been tested. By utilizing RSUs as traffic lights in a centralized system, pedestrians could be integrated into the VTL paradigm. Consequently, the RSU transmits the corresponding virtual light value to pedestrians and vehicles via V2I and P2I communication. The use of infrastructure communication could be a key component of distributed traffic management. Installed RSUs communicate with nearby pedestrians and vehicles via P2I and V2I, and collect data to share with RSUs. The RSUs can communicate indirectly with each other and avoid collisions by sending and receiving Cooperative Awareness Messages (CAMs) only from the RSU. In addition to detecting pedestrians, the RSU can also interact with occluded vehicles using its sensors [13].

4. **Information processing unit**
Electronics, communications, and information processing comprise Intelligent Transportation Systems (ITS) in order to increase the efficiency of the transportation system [6]. Information processing is a crucial component of ITS. ITS relies heavily on the information processing unit, which collects, analyzes, and interprets data from various sources. Traffic control, incident management, and route optimization are just a few of the ITS uses for the information processing unit [27]. Traffic Management Systems (TMS) collect data from connected system components, process them, and inform road users about traffic conditions. The gathered data is processed so that services and applications can be developed. As a VRU protection system, a TMS permits the collection and dissemination of information about VRU presence over a broader area than an individual unit of equipment on the roadside. This

may be appropriate for example in the situation of a highway where vehicles drive at high speeds and need to be warned of a potential collision earlier compared to a rural road, or in smart cities where monitoring specific areas allows drivers to be informed when a march is taking place on a particular street. In addition, machine learning, especially deep learning, has played a crucial role in ITS because it allows data to be processed enormously [15]. Information processing units can improve transportation safety, efficiency, and sustainability by integrating advanced communications technologies, such as sensors into vehicles. In summary, ITS is dependent on the information processing unit, which makes it more efficient and intelligent.

3 Pedestrian to Infrastructure Communication System

3.1 Communication Technologies

In the design of P2I systems, a variety of communication technologies have been used. Systems have some features that are largely determined by the communication protocol used. These characteristics include communication range, P2I device choice, infrastructure availability, etc. The characteristics of each communication technology are briefly discussed in this section.

- **802.11p IEEE:**
  The 802.11p standard runs at 5.9 GHz and was designed specifically for V2X communication. It is possible to transmit safety messages within a typical mobile environment with small latency and efficiency. There is a problem in that 802.11p compatibility is a requirement for VRU devices. While Reference [16] demonstrated that smartphones can be configured to support 802.11p, we are unaware of any smartphones or other VRU devices that support 802.11p. There may be problems with deployment as a result, 802.11p-based systems typically provide communications over a distance of one kilometer, providing sufficient coverage even at extreme speeds. There are two kinds of systems based on 802.11p: ones with infrastructure [19,20] and those without [16–18]. P2I safety applications benefit from 802.11p technology because of its reliability and low latency.
- **Cellular:**
  There have been a few attempts to develop P2X safety systems using cellular technology [8,21]. As a VRU device, smartphones are used for communication using 3G or Long-Term Evolution (LTE). The use of central infrastructure in cellular-based P2V systems typically extends the communication range. To determine their suitability for P2I safety systems, cellular P2I systems must be investigated further in terms of their latency and scalability performance. Mobile systems are a good candidate for P2I convenience applications because of their wide coverage and high market penetration. As part of the proposed 5G architecture, cellular V2X and P2X are currently under development.

- **Wi-Fi:**
  There have been several efforts to design P2X safety systems established on Wi-Fi [22,23]. The systems typically use a smartphone or smartwatch as the VRU device, and their communication range is 100 to 150 m. Typical vehicle speeds in urban areas are 50 kmph, so this range may be sufficient. As a result of the smaller amount of time offered for the vehicle driver to react to crash indicators in suburban areas with standard speeds of 100 kmph, it may not be sufficient. Due to the mobility of vehicles, Wi-Fi connection requirements are also challenging, as it may take too long for safety messages to be exchanged.
- **Bluetooth:**
  System for bicyclists that uses Bluetooth-based indirect P2I communication. Using iBeacon as VRUs, this system communicates directly with the vehicle. This system reaches a communication distance of up to 50 m, which may be sufficient in some pre-crash scenarios. Bluetooth, however, cannot support V2P completely due to its restricted communication range but it supports the P2I system. For example, the system may support only slow urban scenarios [7].
- **700 MHz ITS Band:**
  An ITS system uses 700 MHz for V2P communication (according to FCC,US Standards) [24]. A variety of channel access mechanisms are evaluated for a V2P system. Pedestrian safety can be improved in a number of ways by using the 700 MHz band for P2I communication. When crossing the street, pedestrians could receive real-time updates about weather conditions and traffic, which could help them be safer and more informed. However, implementing P2I communication using the 700 MHz band would require significant infrastructure investments, such as installing sensors and other equipment in traffic infrastructures as well as developing new wireless networks. P2I communication in the 700 MHz band could be beneficial, but implementation of such systems would require careful planning and coordination [25].
- **802.15.4:**
  Low-rate wireless personal area networks (LR-WPANs) use the IEEE 802.15.4 wireless communication protocol. A variety of frequency bands are supported, including 2.4 GHz, 915 MHz and 868 MHz [9]. Low power consumption is one of the advantages of using the 802.15.4 standard for P2I communication, which makes it ideal for battery-powered sensors and other low-power devices. The 802.15.4 standard also supports low data rates and short-range communication, which is helpful for P2I applications that require real-time communication and low latency.

3.2 Types of Safety Related Messages in ITS

The purpose of this subsection is to highlight the types of communication messages used in the VRU protection use case. There are multiple factors that may be included in general safety messages, such as the direction of the vehicle or pedestrian, speed, and location. Recipients can use this information to detect pedestrians, track pedestrians, and predict pedestrian trajectories. Messages received by the system allow it to operate effectively. The implementation of safety message standards for VRUs has been described in several case studies recently [27].

- **Cooperative Awareness Message (CAM)**
  Users of the road exchange safety-specific messages frequently with the surrounding area. These messages, called Basic Safety Message (BSM) in the Society of Automotive Engineers (SAE) standard or CAM in the ETSI standard, contain context-aware information (e.g., Vehicle type, vehicle ID, vehicle position, heading angle, speed, lateral and vertical acceleration, etc.) [28]. Vehicles can transmit a safety message at a frequency of 10 Hz (i.e., at a fixed frequency). The frequency at which safety messages are transmitted by VRUs may vary. There are a number of factors that may affect frequency, including location and speed. CAM contains the following containers: ITS PDU Header, Generation Delta Time, Basic Container, High-Frequency Container, Low-Frequency Container, and special Information Container. Among these containers, the Low-Frequency Container and special Information Container are optional in the message, whereas the others are mandatory and must be included in every CAM. The CAMs generated by a vehicle must include a high-frequency vehicle container (Vehicle HF) and a low-frequency vehicle container (Vehicle LF). Information about the vehicle's speed and heading may change quickly (dynamically) in the Vehicle HF container. There is a container for Vehicle LF that holds static or slowly changing information about the vehicle, such as the status of the exterior lights. A vehicle with a specific function in road traffic, such as a public transportation vehicle, must provide updated status information in special containers. This includes traffic rules, hazardous goods basics, and emergency priority.
- **VRU Awareness Message (VAM)**
  A VRU connected to a smartphone is able to send a message. Compared to CAM, this message type is more flexible. This type of message is characterized by its short length and context-specificity. The ETSI standard [27] introduces the VAM message, and the SAE standard introduces the Personal Safety Message (PSM). It contains information about the location, type of VRU, speed, and direction of the VRU. The VRUs are responsible for generating and constructing VAMs, along with motion prediction and other contextual information to increase position accuracy. In the VAM, the following containers are included: ITS PDU Header, Generation Delta Time, Basic Container, High-Frequency Container, Low-Frequency Container, Cluster Information Container, Cluster Operation Container, and Motion Prediction Container. Among these containers, Low Frequency Container, Cluster Information Container, Cluster Operation Container, and Motion Prediction Container are optional when sending a message, others are mandatory and must be included in every VAM. A cluster container in VAM is a unique approach to optimizing spectrum resources compared to existing V2X message types defined by ETSI. A cluster is formed by combining VRUs with homogeneous behavior

[16]. Clusters have a leader who transmits VAMs. VAM dissemination rules determine at what frequency VAMs are transmitted. 1 Hz is the minimum frequency and 5 Hz is the maximum frequency.

- **Decentralized Environmental Notification Messages (DENM)**
DENMs that alert users to risks of VRU crashes are event-driven messages that are triggered only when hazardous events occur. A DENM message contains information about the severity and location of the event. DENMs must always include the ITS PDU header and the management container. Optional containers include the situation container, the location container, and the à la carte container. The situation, location, and à la carte containers must not be present for a cancellation DENM or a negation DENM. The location container must be present if the situation container is present. A la carte containers are presented only when they are specified in application specification standards, such as ETSI TS 101 539-3 [i.6], ETSI TS 101 539-2 [i.5] and ETSI TS 101 539-1 [i.4] [27]. There are two types of containers: data elements (DE) and data frames (DF). You can either choose to have a DE and a DF or you can make them mandatory.
- **Cooperative Perception Messages (CPM)**
Using CPM, vehicles exchange sensing information to improve their perception of their environment while driving. Information about detected objects in the surrounding area is contained in them. For them, the ETSI Standard specifies the format, generation, and transmission rules [29]. The conditions of the detected object are updated every 1 s or as soon as they change. In the current implementation of ETSI-CPM, high-frequency transmissions of CPMs are common, but the CPMs only contain a small amount of information about the detected objects. In [30], authors have proposed an improved CPM generation algorithm that predicts the behavior of detected objects to optimize the generation rules. As a result of their approach, CPMs are transmitted less frequently but contain a greater number of detected objects per CPM. It consists of an Intelligent Transport Systems (ITS) Protocol Data Unit Header (ITS PDU Header) and CPM parameters [26]. There are four main containers in CPM's payload: Management Container, Station Data Container, Sensor Information Container, and Perceived Object Container. Data contained in the Management Container and Station Data Container describes the type of sender station, such as a vehicle or a Road-Side-Unit (RSU), as well as the actual orientation angles, position, heading of the vehicle, and dynamic. Information about sensors attached to a sender is inserted into Sensor Information Container, such as LIDARs, radars, cameras, and their capabilities, such as ranging opening angles, or location where they are placed. A list of objects detected is stored in the Perceived Object Container, which contains information about their speed, dimensions, relative position, and acceleration. If the trigger conditions are met, the message must be transmitted with a minimum frequency of 1 Hz and a maximum frequency of 10 Hz, according to CPM generation frequency management.

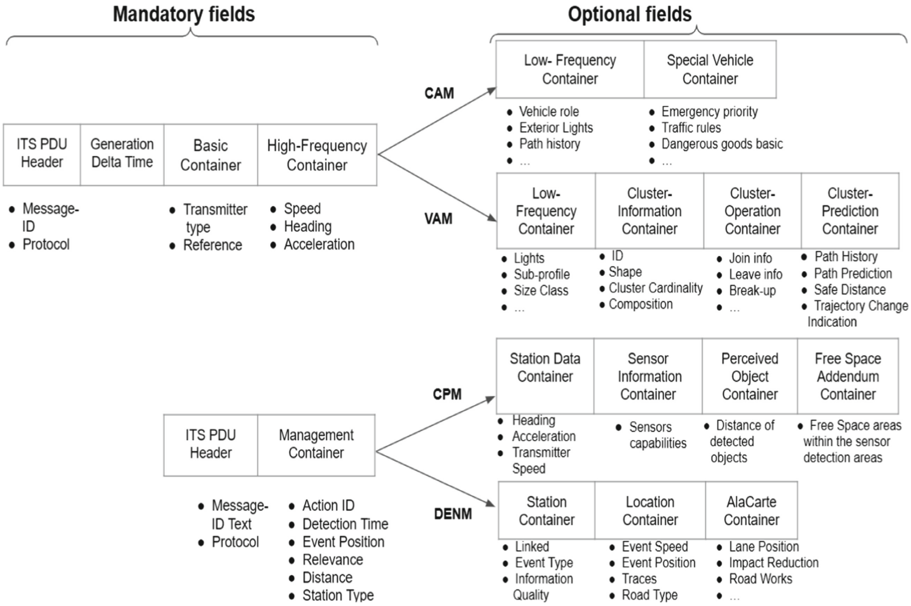


Fig. 2. ITS message formats [14]

A representation of the different fields in the messages discussed above is shown in Fig. 2. In this regard, the mandatory fields in VAM and CAM messages are similar to CPMs and DENMs. Safety messages or awareness messages play a crucial role in collision avoidance because the VRU participates actively by sending VAMs to the servers and vehicles as part of the communication process. Additionally, they may participate passively through other vehicles detecting them and including their data in CPMs or DENMs (e.g. in the collision risk field). Communication messages are not the only data collected during the data collection phase. The system can be extended to collect data from multiple sources (e.g., data from road cameras, sensor data, network data, and self-positioning of VRUs). The collision avoidance application can be placed on a server or run directly on the smartphone of the VRU or vehicle. Our survey considers ITS messages as the most important source of information to improve pedestrian safety.

3.3 Pre-crash Scenarios

In this subsection, we will explore a pre-crash scenario of pedestrian-to-vehicle communications through infrastructure (RSU). Figure 3 illustrates the pre-crash scenario of communication between pedestrians to vehicles Via Infrastructure (RSU). An overview of pedestrian-to-vehicle (P2V) communications through an infrastructure (RSU). Communication between an RSU and a vehicle, or an RSU and a pedestrian, can approximate P2V communications. Communication devices, such as traffic signals, are referred to as RSUs. Pedestrians hold communication devices (e.g., smartphones) and approach an intersection from a point that is out of the line of sight of vehicles. Pedestrians and vehicles are assumed to be separated by structures, making direct communication impossible. As a result, an RSU is used to share the location of a vehicle and a pedestrian to prevent collisions. Here are the details regarding the pedestrian and the roadside unit. RSUs are capable of communicating via WLAN and LoRaWAN. The device acts as both an access point (AP) for WLAN and a gateway (GW) for LoRaWAN. As it is connected to the backbone network, it is capable of determining the location of vehicles in its vicinity. There is the possibility of a pedestrian holding a device that communicates via WLAN and LoRaWAN. In addition to supporting WLAN and LoRaWAN, it also serves as an end device. GPS data is obtained from the device's built-in GPS. It should be noted that GPS measurement errors are not taken into account. The P2I systems for VRUs can communicate with the infrastructure and vehicles. Vehicles and pedestrians exchange information indirectly, through infrastructure. A couple of examples of P2I systems for VRUs that involve indirect communication are discussed in references [8,19]. Devices may utilize the same technology, such as cellular communication [29], or they may use different technologies, such as Wi-Fi and 802.11p [19]. An indirect mode that involves multiple hops can be viewed as a variation. The use of multi-hop communication may be advantageous in non-line-of-sight crash situations. Vehicles can rebroadcast safety messages they receive from VRUs to other vehicles around them. For example, public transport buses might broadcast safety messages about VRUs passing the street next to them at bus stops. A message exchanged through the infrastructure may be processed by infrastructure nodes before being forwarded to other nodes. In this case, high computing power may be required on the infrastructure nodes. Also, the latency of communication may be higher when messages are exchanged through infrastructure nodes. To accomplish this, the pedestrian or vehicle application's latency requirement must be

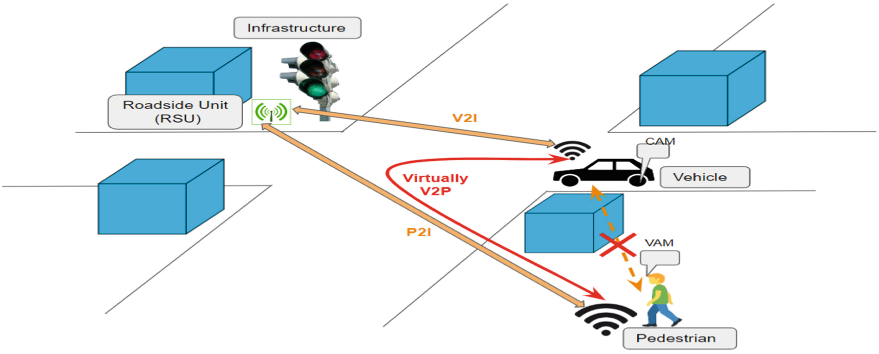


Fig. 3. An overview of the P2V communication Via Infrastructure (RSU) [31]

compared to the infrastructure's latency. It may be helpful to use pre-crash scenarios to better understand the requirements for effective pedestrian-to-vehicle (P2V) communications through an infrastructure (RSU) crash prevention system. There may be differences in the pre-crash scenarios for various types of VRUs. Also, most pedestrian accidents occur at non-junctions.

4 Pedestrian to Infrastructure System Requirements

P2I communication systems require meeting a set of requirements, so understanding the application and technical requirements is crucial for the implementation of better pedestrian safety approaches. The following sections outline key requirements for P2I communication in accordance with the VRU safety standards developed by ETSI [27,34]. A pedestrian safety application can be generally categorized into two types of application: 'Convenience or Awareness' is the simplest and 'Safety' is the most advanced [35]. By providing basic safety notifications, awareness applications inform other road users of their presence to maintain cooperative awareness. The VRU positioning and speed data are not very accurate for such applications, but basic status data will need to be broadcast on a periodic basis between vehicles and VRUs. Alternatively, collision avoidance applications calculate road user paths to generate collision risk warnings; as a result, such applications rely on highly precise vehicle positioning and precise information about its speed, heading, and direction of travel. Considering these differences, it is important to identify the main requirements for P2I implementation. In order to achieve this, we have recognized seven parameters that must be met for a functional VRU communication system.

- **Communication latency:**
  In data communication, end-to-end latency is an important parameter to minimize because it carries time-sensitive and safety-related messages that decide the accuracy of control messages. The shared information needs to be timely enough so that the receiver can use it for collision avoidance, so a minimal end-to-end latency should be achieved (e.g., less than 300 ms) and a sufficiently high sampling rate (e.g. 10 Hz) must be implemented [27,37,38].
- **Position accuracy:**
  P2I application and safety warnings are generally based on road user location; accordingly, it is crucial to know the exact location of the user. VRU applications require a significantly higher level of positioning accuracy than conventional CITS applications. Currently, smartphone positioning systems are not accurate enough to provide a reliable source of localization. They must be improved to provide centimeter-level accuracy. A position accuracy of 1m is required for vehicle applications based on European standards [36]. When determining whether a VRU is located in a secure area, however, measurements must be significantly more precise and accurate [33].

- **Scalability:**
  Applications that avoid collisions or provide awareness should be able to cope with multiple road users (500 to 5000 in the same communications zone, or within 300 m, as described in ETSI 103-300-2 [27]). By using an effective clustering approach, a VRU system can cluster active users within a geographic area.
- **Communication range:**
  P2I communication has the benefit of detecting hazardous situations before visual contact is made. In order to prevent conflicts, early warnings, and precautions must be taken to detect them in time. To provide the appropriate time for the warning, it is necessary to consider Time-To-Collision (TTC) as well as the user's response time, the time required for maneuvers, communication latency, and a safety margin [35]. The range must be broad enough so that a risk assessment can be made based on the awareness messages before the warning is issued.
- **Warning message design and user interface:**
  Users of VRU safety applications should benefit from a user interface that provides clear and straightforward information, minimizes distractions, and reduces content and workload [32]. Road users deserve to be alerted to safety warnings when they need to be without being distracted by frequent false alerts or low-risk warnings. In order to determine the appropriate timing for delivering warning modes and warning messages to drivers and VRUs, it is necessary to take into account both the type of VRU and the level of danger.
- **Context awareness:**
  In the context of collision avoidance systems, refer to various pieces of information that the system needs to operate effectively and avoid collisions. This includes information about the environment, such as the position and speed of other vehicles, pedestrians, and obstacles. It also includes information about road conditions and weather. Collision-avoidance systems are designed to identify movements (momentums and trajectories) so that they can be acted upon promptly (reducing velocity or changing trajectory) in order to prevent collisions [27,34]. By using sensors on the VRU devices, it is possible to determine the environment and the movement of VRU object states (such as standing, walking, jogging, cycling etc.) with such applications [35]. Therefore, movement prediction should be highly accurate in order to minimize conflict miscalculations.
- **Security and Privacy:**
  VRU applications generate security and privacy concerns, requiring mitigation strategies. The issue of false positives and false negatives is a legitimate security concern.

  The term **false positive** relates to a situation in which the receiver believes there is a need to act even though no such situation exists. It takes place when a recipient accepts information in the VRU system as truthful when it is misleading. The receiver may be induced to take action in the real environment as a result of such a situation, negatively affecting system users. As an example, when a false VRU message offers a vehicle driver with the erroneous perception that a youngster was jogging in the way of the vehicle, that may cause a rear-end collision because the driver unexpectedly hits the brakes [34].

A **false negative** happens when the receiver does not believe that a reaction is necessary when the situation actually happens. Receivers may experience this either when they do not receive the relevant warning message or when they receive conflicting messages that undermine their belief in the original message. It is possible, for instance, for a receiver not to receive any messages from VRUs because of a denial of service (DoS) attack. To prevent false positives, VRU communications must include cryptographic protection with authorizations only granting access to trusted devices [34]. Nonetheless, communication security mechanisms alone cannot protect against false negatives. An example of such an attack would be a DoS attack. This is an unavoidable condition, though, it can theoretically be recognized and the authorities notified of the attack so that it can be mitigated physically. An attack based on contradictory messages can also be prevented with communication security mechanisms that make it more difficult for invalid senders to generate convincing contradictory messages. Furthermore, VRU apps may lead to privacy questions as they gather personal information about other road users and VRUs. It is therefore important to implement technical methods to secure the data of other road users when mitigating privacy concerns. It may be necessary to restrict the inclusion of critical personal data in messages or to periodically change the identifiers assigned to temporary senders. In addition, data management strategies regarding the retention and access of data generated by VRU applications need to be integrated into mitigation strategies that address privacy concerns (Table 1).

5 Pedestrian-to-Infrastructure System Design Challenges

- **Real time detection:** Real-time information is extracted from moving objects by the human visual system. It can autofocus on various objects in its surrounding environment without undergoing any behavioral changes. It is difficult for the camera to detect obstacles without optical flow or motion parallax. Tracking other objects is essential (e.g., nonhazardous obstacles, possible flying objects, etc.). Although camera technology has advanced, it remains challenging to observe multiple objects concurrently at low levels. The fact that tasks considered easy by humans are challenging in computer vision means that humans are capable of recognizing a person regardless of the vehicle's orientation, angle of view, or even several vehicles together. In spite of this, object detection methods face numerous problems, such as illumination conditions, occlusion, viewpoint variation, etc. A common street scenario is the occlusion of two or more objects when they are too close together and appear to blend or merge. In addition to accuracy, speed is an important factor, which means that algorithms that detect objects in motion

Table 1. Summarizes the technical requirements that are described from the above sections for the P2I communication system based on the ETSI standards.

Basic Requirement	Requirement Value
Communication Latency [37,38]	The latency should not exceed 300 ms but be below 100 ms
Position accuracy [27,36]	Precision of at least 0.5 m is required
Scalability [27]	It should be able to handle urban scenarios involving up to 5000 users per intersection.
Communication range [35]	Range ≥ 25 m when P2I communication is used to protect the VRU. Range ≥ 70 m range when P2V communication is used for pedestrian collision avoidance purposes (at (45 km per hour, stationary pedestrian and vehicle).
Warning message design and user interface [33]	An optimal user interface should deliver information in a straightforward manner with minimal distractions, and be designed to reduce workload and content.
Context awareness [34,35]	VRUs should be able to predict movements accurately enough to minimize conflict miscalculations.
Security and privacy [34]	In order to prevent false positives, messaging needs to be protected by cryptography. To prevent false negatives, identifying the attack source and physically removing it is necessary. In order to prevent privacy issues, messages should not contain critical personal information, or temporary sender identifiers should be changed regularly

must accurately identify important objects. This challenge can be overcome by mapping technologies and computer vision, such as concurrent detection [39] and tracking and deep learning and machine learning [40].

- **Insufficient information:** For detecting a potential collision, it is necessary to have detailed information about the objects such as their size, position, material, speed, etc. To identify objects, characterize them, and determine their distances from pedestrians, safety systems must have detailed information. The system gathers this information based on coarse-grained data without considering materials, nature, and intentions. There is insufficient data to detect collisions accurately based on such data. An example would be the angle at which objects are positioned, the surrounding environment, the type of obstacles, etc. Using Geographic Information Systems (GIS), safety systems can gather data about the surrounding areas in advance. For example, the presence of VRUs in schools and recreation facilities is possible. It is possible for a safety system to make a decision based on those data and to warn pedestrians/drivers in advance if it has those data.
- **Hardware limitation:** Sensors are integrated into smartphones and wearables for restricted computation power and functions. It is true that these sensors are sufficient for everyday activities, but they do not provide high accuracy when it comes to detecting obstacles. For example, the common smartphone is mainly built for daily use and is not integrated with specific sensors. There are a limited number of speakers and microphones on the device. In contrast, sonars and radars are specially developed and configured with various receivers and transmitters. When pedestrian safety is concerned in an urban area, granular level accuracy is often required in a matter of seconds [41]. The current generation of smartphones and wearables are low-powered so large data cannot be handled by these systems. A smartphone GPS can also be considered a hardware limitation. Battery drain will be significant if we want accurate positioning accuracy.
- **Human factor:** Due to inconsistency, human factors play an important role in collision detection systems. Inter-pedestrian/social behavior, pedestrian body posture, and pedestrian consciousness all affect pedestrian safety. Every human is distinct from these factors. A number of studies have explored pedestrians' contours, postures, and body language [42,43]. It is even more difficult to estimate pedestrians' movements because their impending motion is uncertain. System safety can be improved by adapting trajectory prediction [44]and activity recognition [45].
- **Dynamic environment:** In the real world, pedestrian safety is challenging due to a dynamic environment, especially in cities. Streets in cities, vehicle traffic, and crowded pedestrians pose different safety problems every time. The majority of research detects static obstacles in this dynamic environment, but not moving obstacles. As a result of recent developments in Simultaneous Localization And Mapping (i.e., Dynamic SLAM) and robotics technologies, this problem has been overcome [46,47].
- **Noisy sensor data:** Detection of obstacles is challenging due to noisy sensor data and environmental disturbances. Initially collected data contains noise caused by unexpected body or hand jitters, affecting accuracy. The sensors built into smartphones, for example, require calibration, and filtering, and are unable to distinguish between different motions. Similarly, noise

adversely affects acoustics and inertial sensors. When noise is present in data, it can make the processing more complex and take longer, which can negatively affect performance. Detection systems should be able to distinguish between various types of sounds. For example, environmental noises (e.g., human sound, non-hazardous sound, walking-induced noise, etc.) and desirable input signals need to be differentiated correctly. In order to handle these noises, a number of filters and techniques were proposed [48,49]. There are multiple levels of noise in deep learning, such as noise at the class level and noise at the feature level. As a result of noise overfitting the model, poor generalization performance was observed in previous research [50]. The relabeling of noisy data has been suggested by some research; however, this technique works best with data collected in static environments [51,52]. Recent studies have shown that noise-resistant object detection can be achieved [53].

- **Sidewalk:** Data on sidewalk accessibility plays an important role in pedestrian safety and obstacle detection. In order to improve accuracy, data quality is important. A city's transportation department typically inspects sidewalks in person through in-person audits. Although, this procedure is time-consuming and costly; the most important part is that it does not occur very often. As a result, these data cannot be used to detect potential dangers in real time by safety systems. In spite of the fact that map service providers offer pedestrian-focused features, there is no information about accessibility on sidewalks. To detect obstacles on sidewalks [54], researchers have used a small set of data [55,56].

6 Conclusion

Modern cities are rapidly developing and the number of vehicles is increasing; therefore, more investment in modern technology is needed to deal with the growing issues related to such growth. Intelligent transportation systems ensure vehicle and pedestrian safety. The majority of developed solutions relied on V2X communication while P2X was less implemented because it was harder to implement and required maintenance. The paper discusses P2I communication systems components and their design challenges. The pedestrian-to-infrastructure communication area of ITS has the potential to improve pedestrian safety, mobility, and overall transportation efficiency. The review found that many studies have used IoT devices such as sensors, smartphones, and other technologies to track pedestrian movement and provide real-time feedback. In order to improve pedestrian safety and mobility in urban areas, more research is needed to identify best practices and develop integrated systems. The future focus of our work will be on deploying, operating, and maintaining a large-scale P2I system using such a comprehensive framework.

References

1. National Center for Statistics and Analysis: 2018 fatal motor vehicle crashes: Overview. Traffic Safety Facts Research Note. Report No. DOT HS 812 826 (2019)
2. Chen, L., Englund, C.: Cooperative intersection management: a survey. IEEE Trans. Intell. Transp. Syst. **17**(2), 570–586 (2015)
3. Dzulkurnain, Z., Mahamad, A., Saon, S., Ahmadon, M., Yamaguchi, S.: Internet of Things (IoT) based traffic management & routing solution for parking space. Indones. J. Electr. Eng. Comput. Sci. (IJEECS) **15**(1), 336–345 (2019)
4. Gandhi, T., Trivedi, M.M.: Pedestrian protection systems: issues, survey, and challenges. IEEE Trans. Intell. Transp. Syst. **8**(3), 413–430 (2007)
5. Malik, R.Q., et al.: Mapping and deep analysis of vehicle-to-infrastructure communication systems: coherent taxonomy, datasets, evaluation and performance measurements, motivations, open challenges, recommendations, and methodological aspects. IEEE Access **7**, 126753–126772 (2019)
6. Liu, W., Muramatsu, S., Okubo, Y.: Cooperation of V2I/P2I communication and roadside radar perception for the safety of vulnerable road users. In: 2018 16th International Conference on Intelligent Transportation Systems Telecommunications (ITST), pp. 1–7. IEEE (2018)
7. Merdrignac, P., Shagdar, O., Nashashibi, F.: Fusion of perception and V2P communication systems for the safety of vulnerable road users. IEEE Trans. Intell. Transp. Syst. **18**(7), 1740–1751 (2016)
8. Hernandez-Jayo, U., De-la Iglesia, I., Perez, J.: V-alert: description and validation of a vulnerable road user alert system in the framework of a smart city. Sensors **15**(8), 18480–18505 (2015)
9. Lewandowski, A., Bocker, S., Koster, V., Wietfeld, C.: Design and performance analysis of an IEEE 802.15.4 V2P pedestrian protection system. In: 2013 IEEE 5th International Symposium on Wireless Vehicular Communications (WiVeC), pp. 1–6. IEEE (2013)
10. General Motors: GM developing wireless pedestrian detection technology. GM News 26 (2012)
11. Teixeira, P., Sargento, S., Rito, P., Luıs, M., Castro, F.: A sensing, communication and computing approach for vulnerable road users safety. IEEE Access **11**, 4914–4930 (2023)
12. Rapelli, M., Casetti, C., Sgarbi, M.: A distributed V2V-based virtual traffic light system. In: 2020 International Conference on Communication Systems & NETworkS (COMSNETS), pp. 122–128. IEEE (2020)
13. Ojala, R., Vepsäläinen, J., Hanhirova, J., Hirvisalo, V., Tammi, K.: Novel convolutional neural network-based roadside unit for accurate pedestrian localisation. IEEE Trans. Intell. Transp. Syst. **21**(9), 3756–3765 (2019)
14. Zoghlami, C., Kacimi, R., Dhaou, R.: 5g-enabled V2X communications for vulnerable road users safety applications: a review. Wirel. Netw. **29**, 237–1267 (2022). https://doi.org/10.1007/s11276-022-03191-7
15. Haghighat, A.K., Ravichandra-Mouli, V., Chakraborty, P., Esfandiari, Y., Arabi, S., Sharma, A.: Applications of deep learning in intelligent transportation systems. J. Big Data Anal. Transp. **2**, 115–145 (2020)
16. Wu, X., et al.: Cars talk to phones: a DSRC based vehicle-pedestrian safety system. In: 2014 IEEE 80th Vehicular Technology Conference, VTC2014-Fall, pp. 1–7. IEEE (2014)

17. Tahmasbi-Sarvestani, A., Mahjoub, H.N., Fallah, Y.P., Moradi-Pari, E., Abuchaar, O.: Implementation and evaluation of a cooperative vehicle-to-pedestrian safety application. IEEE Intell. Transp. Syst. Mag. **9**(4), 62–75 (2017)
18. Kwakkernaat, M., Ophelders, F., Vissers, J., Willemsen, D., Sukumar, P.: Cooperative automated emergency braking for improved safety beyond sensor line-of-sight and field-of-view. In: Proceedings of the FISITA 2014 World Automotive Congress, Maastricht, The Netherlands, pp. 2–6 (2014)
19. Thielen, D., Lorenz, T., Hannibal, M., Köster, F., Plättner, J.: A feasibility study on a cooperative safety application for cyclists crossing intersections. In: 2012 15th International IEEE Conference on Intelligent Transportation Systems, pp. 1197–1204. IEEE (2012)
20. Anaya, J.J., Talavera, E., Gimenez, D., Gomez, N., Jimenez, F., Naranjo, J.E.: Vulnerable road users detection using V2X communications. In: 2015 IEEE 18th International Conference on Intelligent Transportation Systems, pp. 107–112. IEEE (2015)
21. Liu, Z., Pu, L., Meng, Z., Yang, X., Zhu, K., Zhang, L.: POFS: a novel pedestrian-oriented forewarning system for vulnerable pedestrian safety. In: 2015 International Conference on Connected Vehicles and Expo (ICCVE), pp. 100–105. IEEE (2015)
22. Huang, K.S., Chiu, P.J., Tsai, H.M., Kuo, C.C., Lee, H.Y., Wang, Y.C.F.: RedEye: preventing collisions caused by red-light running scooters with smartphones. IEEE Trans. Intell. Transp. Syst. **17**(5), 1243–1257 (2015)
23. Hussein, A., Garcia, F., Armingol, J.M., Olaverri-Monreal, C.: P2V and V2P communication for pedestrian warning on the basis of autonomous vehicles. In: 2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC), pp. 2034–2039. IEEE (2016)
24. Healy, M.D., Healy, D.M.: Federal communications commission Washington, DC 20554 (2012)
25. Nagai, M., Nakaoka, K., Doi, Y.: Pedestrian-to-vehicle communication access method and field test results. In: 2012 International Symposium on Antennas and Propagation (ISAP), pp. 712–715. IEEE (2012)
26. European Telecommunications Standards Institute, ETSI TR 103 562 ITS; Vehicular Communications; Basic Set of Applications; Analysis of the Collective Perception Service (CPS); Release 2, V2.1.1, December 2019
27. ETSI. Intelligent transport system (ITS); vulnerable road users (VRU) awareness; part 2: Functional architecture and requirements definition; release 2. Standard, May 2020
28. Santa, J., Pere n ıguez, F., Moragón, A., Skarmeta, A.F.: Experimental evaluation of CAM and DENM messaging services in vehicular communications. Transp. Res. Part C Emerg. Technol. **46**, 98–120 (2014)
29. ITS ETSI. Intelligent transport system (ITS); vehicular communications; basic set of applications; analysis of the collective perception service (CPS). Draft TR 103 562 V0. 0.15 (2019)
30. Abas, N., Dilshad, S., Khalid, A., Saleem, M.S., Khan, N.: Power quality improvement using dynamic voltage restorer. IEEE Access **8**, 164325–164339 (2020)
31. Oki, N., Mukoda, A., Ueda, A., Fujii, T.: Device adaptive control method considering power consumption for pedestrian-to-infrastructure communications. In: 2022 Thirteenth International Conference on Ubiquitous and Future Networks (ICUFN), pp. 24–28. IEEE (2022)
32. Mans, D., et al.: Recommendations for actions concerning supporting ITS developments for VRUs. Eur. Transp. Res. Rev. **9**, 1–14 (2017). https://doi.org/10.1007/s12544-017-0237-9

33. SAE: Dedicated Short Range Communications (DSRC) message set dictionary. SAE International, Report (2016)
34. ETSI, ETSI TR 103 300-1 v2.1.1: Intelligent Transport System (ITS); vulnerable road users (VRU) awareness; part1: use cases definition; release 2, ETSI, Report (2019). Online. https://www.etsi.org
35. Scholliers, J., Van Sambeek, M., Moerman, K.: Integration of vulnerable road users in cooperative its systems. Eur. Transp. Res. Rev. **9**(2), 1–9 (2017)
36. ETSI, "ETSI TS 101 539-3 v1.1.1: Intelligent Transport System (ITS); V2X applications; part 3:longitudinal collision risk warning (LCRW) application requirement specification," ETSI, Report (2013). Online. https://www.etsi.org/
37. Hasan, K.F., Feng, Y., Tian, Y.C.: GNSS time synchronization in vehicular Ad-Hoc networks: benefits and feasibility. IEEE Trans. Intell. Transp. Syst. **19**(12), 3915–3924 (2018)
38. Hasan, K.F., Feng, Y., Tian, Y.C.: An experimental validation of accurate and precise GNSS time synchronization in vehicular networks. arXiv preprint arXiv:2010.14201 (2020)
39. Bharati, S.P., Wu, Y., Sui, Y., Padgett, C., Wang, G.: Real-time obstacle detection and tracking for sense-and-avoid mechanism in UAVs. IEEE Trans. Intell. Veh. **3**(2), 185–197 (2018)
40. Zhao, Z.Q., Zheng, P., Xu, S., Wu, X.: Object detection with deep learning: a review. IEEE Trans. Neural Netw. Learn. Syst. **30**(11), 3212–3232 (2019)
41. Wang, Y., Chen, Q., Zhu, Q., Liu, L., Li, C., Zheng, D.: A survey of mobile laser scanning applications and key techniques over urban areas. Remote Sens. **11**(13), 1540 (2019)
42. Köhler, S., Goldhammer, M., Zindler, K., Doll, K., Dietmeyer, K.: Stereo-vision-based pedestrian's intention detection in a moving vehicle. In: 2015 IEEE 18th International Conference on Intelligent Transportation Systems, pp. 2317–2322. IEEE (2015)
43. Quintero, R., Parra, I., Llorca, D.F., Sotelo, M.: Pedestrian path prediction based on body language and action classification. In: 17th International IEEE Conference on Intelligent Transportation Systems (ITSC), pp. 679–684. IEEE (2014)
44. Alahi, A., Goel, K., Ramanathan, V., Robicquet, A., Fei-Fei, L., Savarese, S.: Social LSTM: human trajectory prediction in crowded spaces. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pp. 961–971 (2016)
45. Hassan, M.M., Uddin, M.Z., Mohamed, A., Almogren, A.: A robust human activity recognition system using smartphone sensors and deep learning. Fut. Gener. Comput. Syst. **81**, 307–313 (2018)
46. Henein, M., Zhang, J., Mahony, R., Ila, V.: Dynamic SLAM: the need for speed. In: 2020 IEEE International Conference on Robotics and Automation (ICRA), pp. 2123–2129. IEEE (2020)
47. Mohanan, M., Salgoankar, A.: A survey of robotic motion planning in dynamic environments. Robot. Auton. Syst. **100**, 171–185 (2018)
48. Newson, P., Krumm, J.: Hidden Markov map matching through noise and sparseness. In: Proceedings of the 17th ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems, pp. 336–343 (2009)
49. Evans, R., Grefenstette, E.: Learning explanatory rules from noisy data. J. Artif. Intell. Res. **61**, 1–64 (2018)
50. Zhang, C., Bengio, S., Hardt, M., Recht, B., Vinyals, O.: Understanding deep learning (still) requires rethinking generalization. Commun. ACM **64**(3), 107–115 (2021)

51. Lee, K.H., He, X., Zhang, L., Yang, L.: CleanNet: transfer learning for scalable image classifier training with label noise. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pp. 5447–5456 (2018)
52. Li, J., Wong, Y., Zhao, Q., Kankanhalli, M.S.: Learning to learn from noisy labeled data. In: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, pp. 5051–5059 (2019)
53. Xu, Y., Zhu, L., Yang, Y., Wu, F.: Training robust object detectors from noisy category labels and imprecise bounding boxes. IEEE Trans. Image Process. **30**, 5782–5792 (2021)
54. Froehlich, J.E., et al.: Grand challenges in accessible maps. Interactions **26**(2), 78–81 (2019)
55. Najafizadeh, L., Froehlich, J.E.: A feasibility study of using google street view and computer vision to track the evolution of urban accessibility. In: Proceedings of the 20th International ACM SIGACCESS Conference on Computers and Accessibility, pp. 340–342 (2018)
56. Weld, G., Jang, E., Li, A., Zeng, A., Heimerl, K., Froehlich, J.E.: Deep learning for automatically detecting sidewalk accessibility problems using streetscape imagery. In: Proceedings of the 21st International ACM SIGACCESS Conference on Computers and Accessibility, pp. 196–209 (2019)

Computer Vision Based 3D Model Floor Construction for Smart Parking System

Jayaprakash Patra, Satyajit Panda, Vipul Singh Negi,
and Suchismita Chinara(✉)

National Institute of Technology Rourkela, Rourkela, Odisha, India
{jayprakashpatra.23,satyajitpanda002,vipulhld001,suchi.nitrkl}@gmail.com

Abstract. A Smart Parking system has a lot of components, such as an automated parking infrastructure, sensors, and a navigation system. For the implementation of the navigation system in smart parking, a 3D floor map is required. A 3D view of maps is always better than traditional maps, but making a 3D model comes at a cost and requires specialized tools. Infrastructures such as hospitals and offices usually have little luxury when it comes to maintaining their parking spaces, and the proposed system provides a simple yet effective solution for this problem in this paper. Till now, images are two-dimensional, and tools like Lidar or Kinect are used to get the depth element right. However, to make the floor construction handy, portable, and lightweight, a smartphone image-based approach is proposed here to make a 3D model of indoor parking lots. The pillars and the separation walls between parking spaces are easy to identify using deep learning models. A convolution neural network-based architecture was used for object detection. The main problem that remains is to calculate the depth of the objects in the image. Here in this paper, a successful approach is proposed to overcome the problem of finding depth in images.

Keywords: Smart Parking Systems · 3D Mapping · Computer Vision

1 Introduction

With the increased population of vehicles, the developing countries are really in scarce of places to park them in public places like malls [11], airports, hospitals, stadiums etc. Further, the long waiting time for car parking and the pollution generated in one place through the fuel consumption during the parking waiting time are frustrating for the drivers. This demands the need for sufficient parking space, which is difficult to afford in a highly populated country like India. Therefore, the design of smart parking systems (SPS) are more into research and development. One of the major components of the SPS is the smart navigation system that guides or navigates the driver inside the parking lot by providing a floor map of the parking area. Such floor plans of parking locations will enable the drivers to navigate from their current locations to the available parking spaces

D. Puthal et al. (Eds.): IFIPIoT 2023, IFIP AICT 684, pp. 36–48, 2024.
https://doi.org/10.1007/978-3-031-45882-8_3

in real-time. The paper proposes a cost-saving and easy method to generate 3D floor models for indoor SPS.

As per the study conducted in 2019, Indian Vehicles are usually parked for 95% of the time [5]. All those vehicles need parking spaces, but navigating around the parking space without any guidance may consume time and effort. Having a 3D model of the parking space would not only be helpful, but also it will save the time and frustration of the driver as well as save the environment to a great extent. A perfect 3D model requires special hardware tools like LIDAR, RGB-D Camera and Kinect sensors etc. The data gathered from these goes into software such as Blender, OpenSCAD, FreeCAD for 3D modelling. However, these tools and techniques are expensive and needs skilled manpower to install and operate. However, smartphones are everywhere, and they have good cameras, even with the lower-range models. Taking images of an empty parking space is easy and can be done with a simple smartphone without the need for specialized tools.

In the proposed approach, the images are used to create 3D models of parking spaces. The approach is cost-saving as the proposed model can generate 3D models quickly using a single image.

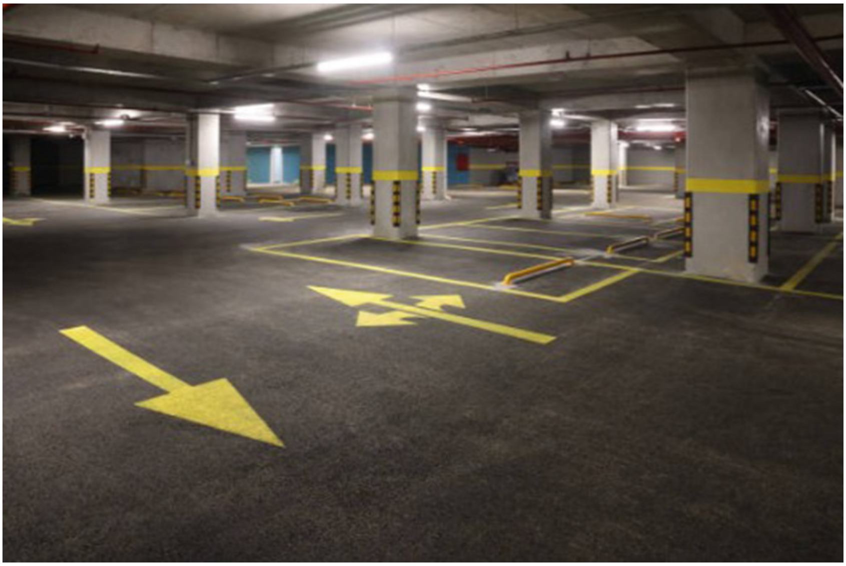


Fig. 1. A simple empty parking lot.

Figure 1 shows an empty indoor parking lot. Upon closer inspection, the walls and the pillars are the primary ingredients of an indoor parking lot because they obstruct a user's vision and navigation into a parking lot. That also includes walls and pillars as a component in the construction of the 3D model. In this proposed work for object detection (Pillars and Walls), deep learning techniques are used. The reason behind opting to use deep learning over traditional machine learning is due to its capability to process unstructured data like documents and images, as it uses complex structures of algorithms modelled on the human brain. It learns high-level features from the input data in an incremental manner. The major challenge of the proposed work is figuring out the depth of the detected object. Images are 2D structures; a third dimension is needed to convert them to 3D. In this paper, a method for getting that depth data is proposed.

In the remainder of this paper, a review of papers in the similar domain has been done in Sect. 2. Section 3 explains the proposed work, which contains the model architecture and system models. Section 4 discusses the implementation and result analysis of the proposed work. Finally, Sect. 5 concludes the paper.

2 Literature Survey

A Smart Indoor Navigation system is required to guide the user in complex indoor areas like malls, offices, and parking lots. For the execution of the Smart Indoor navigation system, it needs a 3D indoor map. Dong et al. [3] proposed that for the implementation of the navigation system, it needs a fine-grained and up-to-date indoor map. The approach here used is to utilize crowd-sourced data to develop an indoor navigation system. It created an indoor navigation system based on the 3d model of the environment. It is usually maintained by photos from various sources and the sensor data collected from the sensors deployed in the interested region. It takes the photos as the input to create the 3D model using SfM (Structure from Motion) techniques and then creates a navigation system based on the obstacle information like walls and pillars.

Traditionally, 3D model construction was done in two phases, the depth estimation of the object and the surface construction. Sayed et al. [9] proposed that a 3D object model is built by the sequence of 2D images without relying on 3D convolution. It is a two-step process in which the first step is to extract the feature from the images using Convolutional Neural Network, and then the next step is to use the feature map to construct the 3D model.

A floor plan depicts a large portion of indoor spatial data like walls, beams, and rooms, but there is a need for an automatic solution for generating high-quality elements like walls and beams. Wu et al. [15] proposed an overview of the different methods and algorithms developed to parse floor plan images and create accurate indoor maps and models. It states that the Internet Mapping Model (IMM) can effectively increase the accuracy of Indoor positioning of elements in an indoor space. The indoor mapping is done in four phases: preprocessing, feature extraction, parsing, and reconstruction.

The Information collection about an object and its mapping is a very tedious task, and it requires data from multiple observation points. Otero et al. [7] propose that there can be the use of mobile devices to collect data from many observation points. The mobile mapping system is classified from each other on the basis of its physical configuration like handheld, backpack, and trolley. The mapping sensor used is a LiDAR (Light Detection And Ranging) or an RGB-D (Red, Green, Blue - Distance) camera.

There are a lot of images of a particular Indoor space that are widely available over the internet. Dong et al. [4] suggest a way to use the images to construct the 3D model. The images have been collected from the internet and used to generate the 3D model using the SfM technique. It presents a framework for extracting relevant features from online images like specific objects and using them to construct a map of an indoor space.

The Kinect sensor is designed for consumers' personal and household use, so the accuracy measurement is not so critical. Khoshelham et al. [6] suggested a way to create the 3D model by analyzing the sensor data, like the accuracy and the depth, calibrated by the Kinect sensor. This sensor simultaneously collects data on colours and depth and integrates them in a coloured point cloud. They mainly focused on the depth data and provided a clear view of the geometric quality of the depth data. They concluded that there is an increase in the random error of depth measurement while the sensor distance from the object is increased.

The 3D model construction from the 2d images is a challenging task in computer vision. SusheelKumar et al. [12] proposed that the 3D model construction can be done by extracting features from multiple 2D images and then using this feature to construct the 3D model. It uses SfM techniques which estimate the camera poses and the 3D points from an image. The SfM approach involves feature detection and matching and computation of 3d maps. The quality of the 3D model generated using 2D images depends on the number of images, the quality of the camera calibration, the accuracy of the feature detection and matching, and also in the quality of the bundle adjustment.

Three-dimensional reconstruction from sparse views is a challenging task in computer vision, and it has many applications in real life, such as in Augmented Reality, Robotics, and also in Autonomous driving. Saxena et al. [8] proposed the process of 3D construction using monocular vision. Monocular vision-based 3-D reconstruction is a technique that uses a single camera to reconstruct the 3-D structure of an object or a scene. The camera is moved around the object, and multiple images are captured from different viewpoints. These images are then used to create the 3-D model of the object.

Mobile robots equipped with thermal cameras have the potential to provide a more efficient and comprehensive solution for thermal 3D mapping. Borrmann et al. [1] propose a mobile robot system for thermal 3D mapping. In this approach, the robot moves through the target area and acquires thermal and depth data. The thermal image data and the depth data are fused together to construct the 3D thermal map by using image processing and computer vision techniques.

Real-time camera tracking and 3D reconstruction is a technique used to estimate the pose and reconstruct the 3D shape of an object in real-time using data from a camera. Bylow et al. [2] propose a method to use the signed distance functions (SDFs) that returns the signed distance between a point in floor space and a surface. It is performed in two steps, i.e. camera poses estimation and 3D reconstruction. The object shape is determined by the SDF and the data from cameras.

There have been multiple works in the area of 3D mapping using various sensors like Kinect sensors and RGB-D sensors and various technologies like SfM and IMM. The above-mentioned paper either requires specialized equipment or a higher computation cost to make a 3D model. This paper proposes a low-cost, image-based 3D indoor mapping so that it will be easy for the user to get the 3D model of the indoor space, like in malls, indoor parking lots, and offices. It uses deep learning techniques to provide a fast and accurate measure of locating objects in images.

3 Proposed Work

3.1 Model Architechture

The MobileNet architecture consists of a series of depth-wise separable convolutional layers followed by point-wise convolutional layers. The architecture of the SSD (Single Shot Detection) MobileNet model is divided into two main parts: the **feature extraction network** and the **object detection network**. The feature extraction network is based on the MobileNet architecture, which is designed to be lightweight and efficient for mobile and embedded devices. The object detection network is built on top of the feature extraction network and consists of several convolutional layers that predict the class and location of objects in the image. This Model is low in size and has proven to be best in cases of image processing and mobile devices. We have used one from the Tensorflow 2 Detection Model Zoo [13] (Figs. 2 and 3).

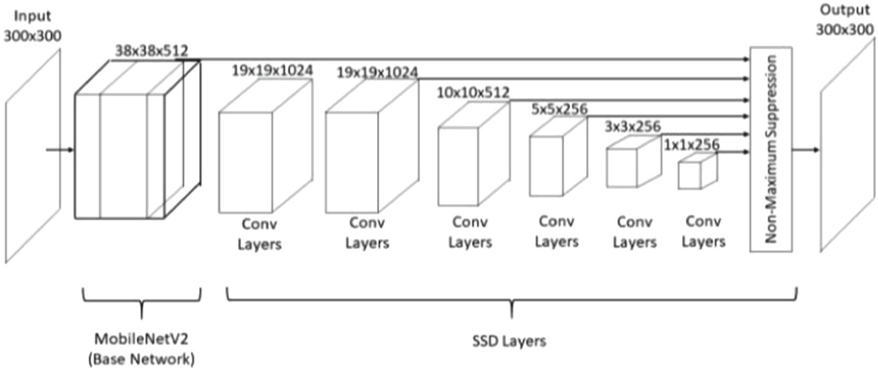


Fig. 2. Architecture of SSD Mobilenet [10].

3.2 System Model

The Proposed Model workflow is used to describe the complete workflow of the proposed work. It is divided into three phases that are given below:

1. Data Input Phase: Contains information about the data collection and dataset preparation.
2. Data Processing Phase: Contains information about the pre-processing and training of the model.
3. Output: Contains the generated 3D model.

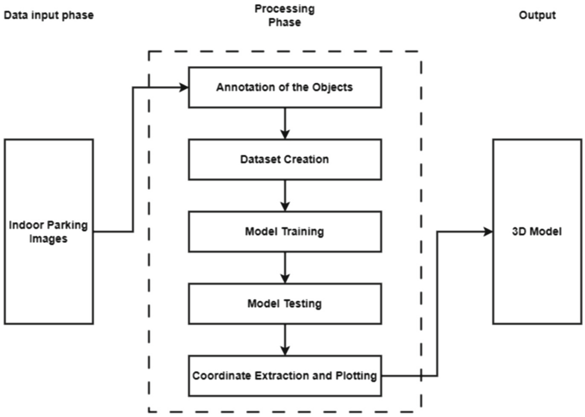


Fig. 3. System Model.

Data Input Phase: In the proposed methodology, empty indoor parking-themed images were first collected by internet scraping [14]. These images were single-shot and included both adequate and low-light conditions. The dataset was prepared by annotating the required objects (Pillar and Wall) from these images only. The dataset size was 140 images, and all the images were converted to 320 × 320 (Fig. 4).

Data Processing Phase: These images were to be class-specified and object-labeled for training and testing of the object detection model to be used. There were several image labelling tools available. Here Open Labeling Annotating tool was used for the object annotation. The Open Labeling Annotating tool provides a PASCAL_VOC XML file as output which contains the details of the bounding boxes, like the max and min coordinates of the bounding boxes. In a parking infrastructure, the major hurdles on the floor are the pillars and the inside wall-like barriers. So, two object classes were considered here, i.e. pillar and wall (Fig. 5).

After getting all the XML files of input images, their information was stored in a CSV file. This CSV file was the created dataset for the object detection model. The CSV file was split into two files, i.e. train_label.csv and test_label.csv, with 80% for training and 20% for testing, as this is the industry standard for

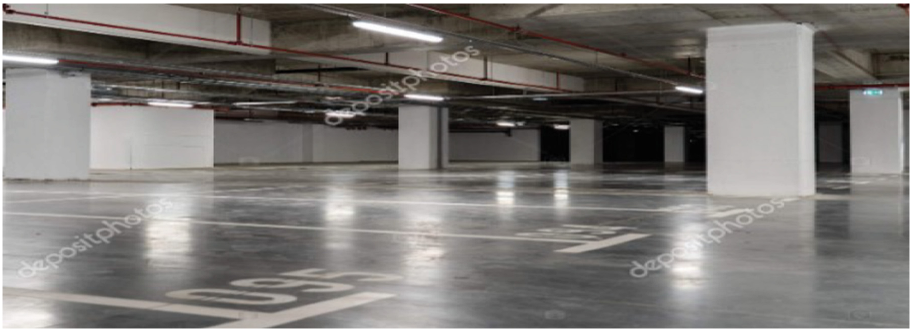


Fig. 4. Sample Image of Indoor parking lot.

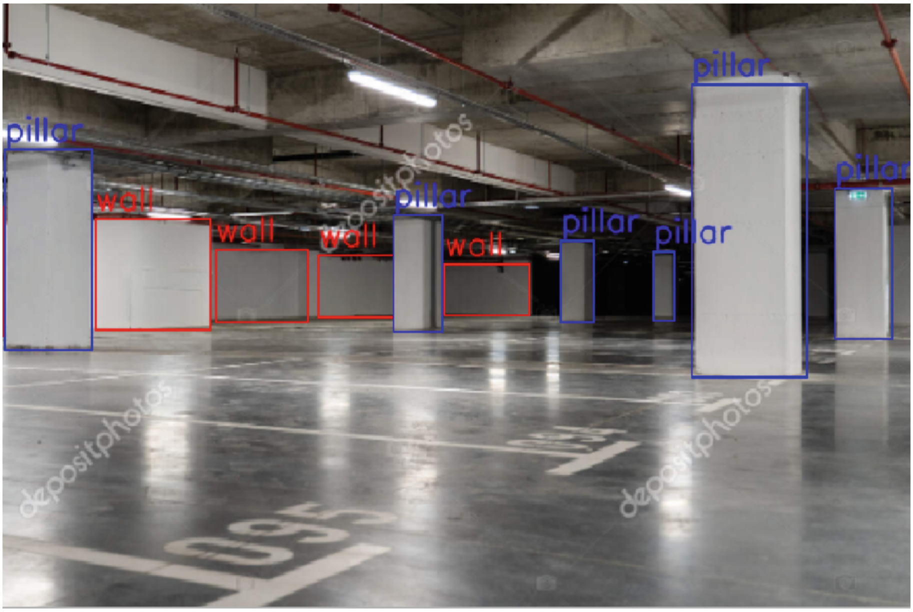


Fig. 5. Annotated Image of Indoor Parking Lot.

splitting data. After that, these CSV files were converted into train and test TFRecord files, respectively. The pre-trained SSD MobileNet V2 [13] FPNLite 320 × 320 model was used for object detection. The train and test TFRecord files were provided as input. The model pipeline config file was obtained, and the class information, batch size, and epoch numbers were updated. The batch size used was eight, and the number of epochs used was fifty thousand.

After the training, model testing was done with the parking image to detect those two class objects (i.e. pillar and wall). The model detected the class objects

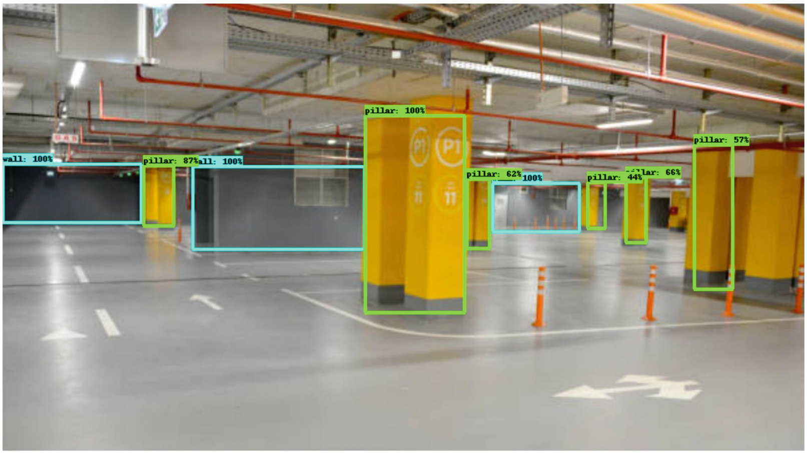


Fig. 6. Output Image with Labelled Objects.

and provided bounding boxes. These detected objects in the image were used for the corresponding 3d reconstruction.

This labelled image was converted into an XML file to get the bounding box coordinates and to plot the objects on a plane; exact positions were obtained. Here, the bounding box coordinates are plotted in the XZ plane, and the depth is depicted by the Y coordinate. From the coordinates of the bounding box, the area of the boxes was calculated using Eq. 1 (Fig. 7).

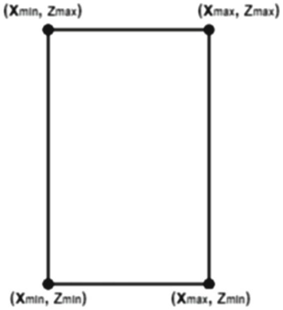


Fig. 7. Coordinates of our Bounding Box.

$$A = (X_{max} - X_{min}) \times (Z_{max} - Z_{min}) \tag{1}$$

Here A represents the area of the object, and X_{min}, X_{max}, Z_{min} and Z_{max} were used to determine the corresponding coordinates of the object.

The general perception used here was when the object is at a longer distance, its area is smaller, so the distance from the viewpoint (D) is inversely proportional to the area of the object (A).

$$D \propto 1/A \tag{2}$$

Output: Matplotlib was used here to plot the objects on a 3D plane. The primary concern here was the relative distance to take between the objects. Considering the backside wall as an XZ plane, the y-axis was taken to provide a relative distance between the objects. So the pillar nearest to the viewpoint was given the lowest positive y-value, and then according to the area ratio, the relative y-values were determined. For the nearest object, an arbitrary one-unit distance was taken. The plotted objects at this stage were now in three dimensions. For an ideal scenario, all pillars were considered the same thickness (the same principle for the walls). Additionally, with Matplotlib, the ipympl library was used to make the plots interactive and to view the 3D plot from various angles for better visualization.

4 Results and Implementation Analysis

A model's entire loss or inaccuracy while predicting item bounding boxes and class labels in an image is referred to as "total loss" in object detection. The loss function is a measure of how far the model's predictions are from the ground truth annotations for a given image. In object detection, the total loss is typically a combination of two types of losses:

- **Localization loss:** This measures the error in predicting the bounding box coordinates of objects in the image.
- **Classification loss:** This measures the error in predicting the class label of the objects in the image.

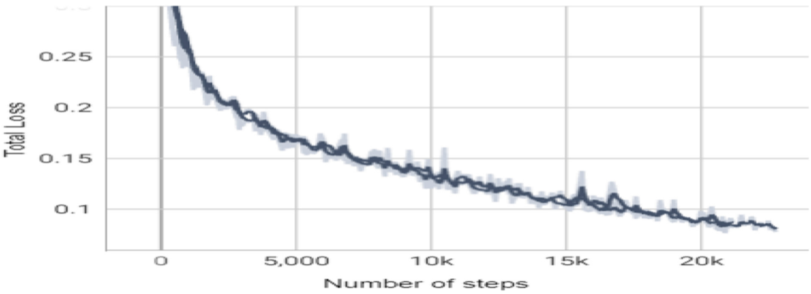


Fig. 8. Total Loss vs Number of steps.

Figure 8 shows the total loss vs the number of steps. The total loss is calculated by adding the localization loss and the classification loss, with the weights reflecting the relative relevance of the two-loss types to the overall task. The goal of training an object detection model is to minimize this total loss; hence the model's accuracy increases.
The term "localization loss" in object detection describes the amount of inaccuracy made when determining the locations of items inside a picture. Object detection models often predict the class of items present in an image and their bounding boxes, which specify the objects' spatial extent. The degree to which the anticipated bounding boxes for each object in the image agree with the actual bounding boxes is known as "localization loss".

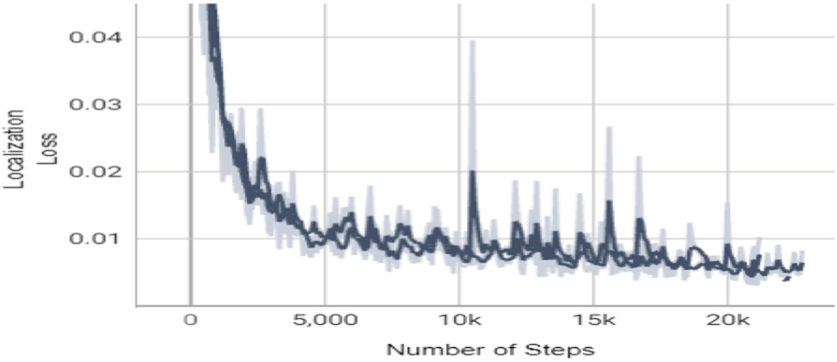


Fig. 9. Localization Loss vs Number of steps.

Figure 9 shows the localization loss vs the Number of Steps. The overall loss function used to train object detection models contains a significant component called localization loss. The model learns to anticipate object positions accurately by minimizing localization loss during training, which enhances the model's capacity for object detection and classification.

In object detection, "classification loss" refers to the amount of error or inconsistency between the predicted class labels and the actual class labels of the objects within an image. In order to recognise items in an image, object identification algorithms often employ a two-stage procedure. The method makes a list of candidate object areas in the first stage, also referred to as "region proposals". In the second stage, the algorithm divides each region proposal into one of the numerous categories, such as "car", "wall", "pillar", etc.

Figure 10 shows the classification loss vs the Number of Steps. The classification loss is often measured using a metric like cross-entropy loss, which assesses the discrepancy between the true class labels for each region proposal and the predicted class probabilities. The classification loss is intended to motivate the algorithm to accurately classify the objects in a picture.
The labelled image was converted into an XML file to get the bounding box

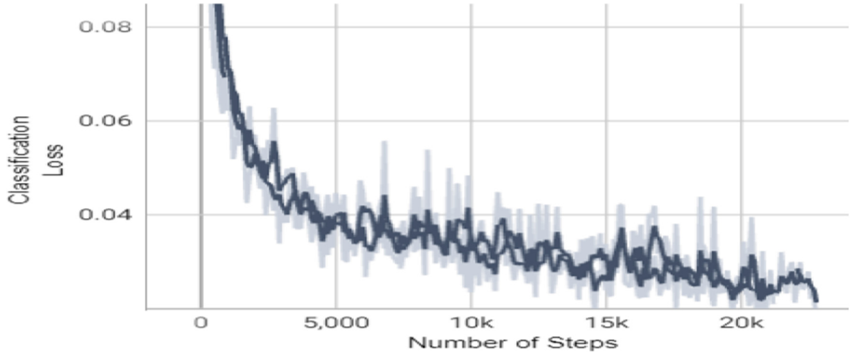


Fig. 10. Classification Loss vs Number of Steps

coordinates and to plot the objects on a plane; exact positions were obtained. Matplotlib was used here to plot the objects on a 3D plane. The primary concern here was the relative distance between the objects. Figure 6 shows the object detected in a sample image, and the below figure shows the different views of the corresponding 3d plot. Figure 11 represents the 3D Models of the parking lot.

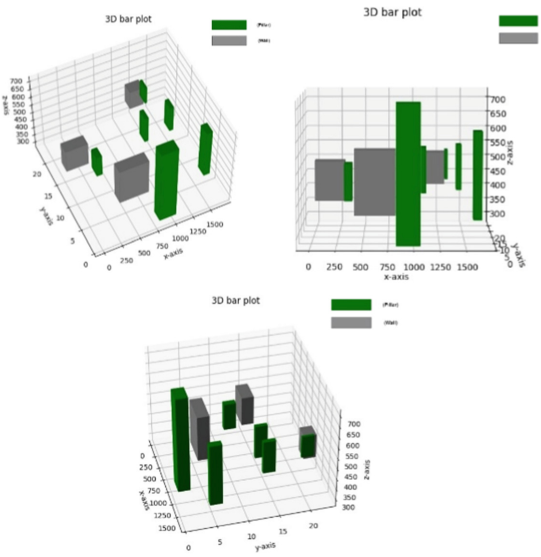


Fig. 11. Front, top, and side view of the 3D Parking Lot Model.

4.1 Result Discussion

The proposed method already provides us with acceptable accuracy, so we focused primarily on reducing the losses. The total loss is around 0.097 if we consider Localization and Classification altogether, while localization loss is at 0.0095, which means that the model is way more efficient in getting the bounding coordinates than getting the box with object classification. The Classification loss is at 0.01, meaning the object detection for pillars and walls is less efficient than our localization (bounding box). This all adds to our total loss. The losses can be further reduced if we gather more data or use a more efficient model than MobileNetV2.

5 Conclusion and Future Works

A 3D model of a smart indoor parking system is done by using an image taken from a smartphone. In order to make floor planning automatic, fast, and reliable, this proposed method is used. This will significantly help out infrastructures such as hospitals, malls and offices. In the future, an appropriate navigation system and a web-based interface to automate the process of converting the images into a 3D model can be implemented as an extension of the proposed work.

References

1. Borrmann, D., et al.: A mobile robot based system for fully automated thermal 3D mapping. Adv. Eng. Inform. **28**(4), 425–440 (2014)
2. Bylow, E., Sturm, J., Kerl, C., Kahl, F., Cremers, D.: Real-time camera tracking and 3D reconstruction using signed distance functions. In: Robotics: Science and Systems, vol. 2, pp. 2 (2013)
3. Dong, J., Xiao, Y., Noreikis, M., Ou, Z., Ylä-Jääski, A.: iMoon: using smartphones for image-based indoor navigation. In: Proceedings of the 13th ACM Conference on Embedded Networked Sensor Systems, pp. 85–97 (2015)
4. Dong, J., Xiao, Y., Ou, Z., Ylä-Jääski, A.: Utilizing internet photos for indoor mapping and localization-opportunities and challenges. In: 2015 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), pp. 636–641. IEEE (2015)
5. India, C.: Pampering Parking: how to manage Urban India's parking needs. http://cdn.cseindia.org/attachments/0.27615500_1518692167_jasolaparkingreport2018.pdf. Accessed 28 Jan 2023
6. Khoshelham, K., Elberink, S.O.: Accuracy and resolution of Kinect depth data for indoor mapping applications. Sensors **12**(2), 1437–1454 (2012)
7. Otero, R., Lagüela, S., Garrido, I., Arias, P.: Mobile indoor mapping technologies: a review. Autom. Constr. **120**, 103399 (2020)
8. Saxena, A., Sun, M., Ng, A.Y.: 3-D reconstruction from sparse views using monocular vision. In: 2007 IEEE 11th International Conference on Computer Vision, pp. 1–8 IEEE (2007)

9. Sayed, M., Gibson, J., Watson, J., Prisacariu, V., Firman, M., Godard, C.: SimpleRecon: 3D reconstruction without 3D convolutions. In: Avidan, S., Brostow, G., Cissé, M., Farinella, G.M., Hassner, T. (eds.) Computer Vision – ECCV 2022. ECCV 2022. LNCS, vol. 13693, pp. 1–19. Springer, Cham (2022). https://doi.org/10.1007/978-3-031-19827-4_1
10. Sheng, T.J., et al.: An internet of things based smart waste management system using LoRa and Tensorflow deep learning model. IEEE Access **8**, 148793–148811 (2020)
11. Statista: Cumulative number of shopping malls in India from 2012 to 2018, with an estimate for 2022. https://www.statista.com/statistics/1211876/india-number-of-shopping-malls/. Accessed 23 Feb 2023
12. SusheelKumar, K., Semwal, V.B., Prasad, S., Tripathi, R.: Generating 3D model using 2D images of an object. Int. J. Eng. Sci. Technol. (IJEST) **3**(1), 406–415 (2011)
13. TensorFlow: TensorFlow 2 detection model zoo. https://github.com/tensorflow/models. Accessed 6 Feb 2023
14. Unsplash: Unsplash. https://unsplash.com/. Accessed 28 Mar 2023
15. Wu, Y., Shang, J., Chen, P., Zlatanova, S., Hu, X., Zhou, Z.: Indoor mapping and modeling by parsing floor plan images. Int. J. Geogr. Inf. Sci. **35**(6), 1205–1231 (2021)

3D Visualization of Terrain Surface for Enhanced Spatial Mapping and Analysis

Pant Shivam[1] and Panigrahi Narayan[2,3](✉)

[1] Micro Genesis TechSoft Pvt. Ltd., Bangalore, India
shivampant158@gmail.com
[2] Center for AI & Robotics, DRDO, Bangalore, India
pani.cair@gov.in
[3] Geographical Information System, Defence Research and Development Organisation, Bangalore, India

Abstract. Visualization of terrain surface finds many applications indifferent area of earth sciences, GIS, and geomatics. With advent of advanced computer graphic algorithms and their HPC implementation through GPU, realistic and high-fidelity visualization of terrain surface is possible. Geographic Information Science (GIS) has made considerable strides since the introduction of 3D terrain visualization facilitating accurate visualization, analysis and measurement of geospatial events and attributes. This paper discusses the significance of different terrain visualization techniques with a special emphasis on 3D visualization.

How 3D terrain visualization is useful in photogrammetry, LiDAR, and aerial imagery, maps can generate detailed models of terrains, buildings, and objects. These techniques enable users to explore geographic features from various angles, zoom in for detailed analysis, and even simulate virtual environments. The applications of 3D maps are diverse and far-reaching. In virtual reality, they can create immersive environments for training, simulations, and gaming. In remote sensing, they aid in understanding natural resources, urban planning, and disaster management. In scientific visualization, they enable researchers to analyze complex spatial data and model real-world phenomena. In GIS, 3D maps enhance spatial analysis, decision-making, and communication of geospatial information.

In conclusion, the evolution of 3D maps in GIS has revolutionized how geographic information is visualized and analyzed, with potential applications in various domains. Advancements in technology continue to drive the development of 3D maps, transforming how we perceive and interact with spatial data, making it more realistic and meaningful.

Keywords: 3D Map · GIS · terrain visualization · photogrammetry · remote sensing · DEM

1 Introduction

Geographic Information System (GIS) has revolutionized the way we collect, store, manage, and analyze spatial data. GIS has been widely used in various fields such as urban planning, environmental management, natural resources, disaster management,

Published by Springer Nature Switzerland AG 2024
D. Puthal et al. (Eds.): IFIPIoT 2023, IFIP AICT 684, pp. 49–63, 2024.
https://doi.org/10.1007/978-3-031-45882-8_4

and transportation. One key aspect of GIS is map visualization, which allows users to interpret and understand complex spatial data in a visual format. Over the years, the evolution of GIS has witnessed significant advancements in 3D map visualization techniques, enabling users to interact with geographic data in more immersive and realistic ways. In this article, we provide a brief history of GIS, discuss the importance of 3D visualization in GIS, and present the purpose and scope of the article.

1.1 History of GIS

Geographic Information System can be traced back to the 1960s when the first computer-based mapping systems were developed. These early systems were limited in functionality and primarily used for data storage and retrieval. In the 1970s, the development of computer hardware and software enabled the creation of more advanced GIS systems, which were used primarily for land use planning and natural resource management. In the 1980s, the introduction of desktop computers and affordable GIS software made GIS more accessible to a wider range of users, including government agencies, academia, and private industries. With the advent of the internet in the 1990s, web-based GIS emerged, allowing users to access and share spatial data over the internet. Today, GIS has become an integral part of many disciplines and continues to evolve with advancements in technology.

1.2 Importance of 3D Visualization in GIS

The introduction of 3D visualization has added a new dimension to GIS, allowing users to visualize and analyze geographic data in three dimensions, which provides a more realistic and immersive experience. 3D visualization in GIS allows users to represent spatial data in a more accurate and intuitive manner, providing insights into the spatial relationships between objects and their vertical dimension. It has become a valuable tool in various fields such as urban planning, architecture, disaster management, and virtual tourism. For example, in urban planning, 3D visualization can help city planners to assess the impact of proposed developments on the surrounding environment and visualize the potential changes in the city's skyline. In architecture, 3D visualization can aid in the design and visualization of buildings and structures in their real-world context. In disaster management, 3D visualization can assist in understanding the terrain and topography of affected areas, aiding in emergency response and evacuation planning. In virtual tourism, 3D visualization can provide virtual tours of natural landscapes and cultural heritage sites, enhancing the visitor experience. The importance of 3D visualization in GIS cannot be overstated as it adds a new dimension of understanding and analysis to spatial data.

1.3 Purpose and Scope of the Article

Purpose of Article

1.3.1 Historical Overview

This subsection aims to provide a brief history of GIS, tracing its development from the early computer-based mapping systems to the present-day web-based GIS. It highlights the key milestones in the evolution of GIS and sets the context for the introduction of 3D map visualization.

1.3.2 Importance of 3D Visualization

This subsection discusses the significance of 3D visualization in GIS, emphasizing its role in enhancing the understanding and analysis of spatial data. It provides examples of how 3D visualization has been applied in various fields such as urban planning, architecture, disaster management, and virtual tourism, illustrating its importance in diverse applications.

Scope of the Article

1.3.3 Review of 3D Visualization Techniques

This subsection provides an overview of the different techniques and technologies that have been used for 3D map visualization in GIS, including photogrammetry, lidar, virtual reality, and augmented reality. It discusses the advantages, limitations, and applications of each technique, providing a comprehensive review of the current state of 3D visualization in GIS.

1.3.4 Applications of 3D Visualization

This subsection presents the diverse applications of 3D visualization in GIS, showcasing examples from various fields such as urban planning, architecture, environmental management, disaster management, and tourism. It highlights the unique benefits and challenges of using 3D visualization in each application domain, providing insights into the practical use cases of 3D visualization in GIS.

1.3.5 Challenges and Future Directions

This subsection discusses the challenges and limitations of 3D map visualization in GIS, such as data integration, interoperability, and usability. It also highlights the emerging trends and future directions in 3D visualization, including advancements in technology, data sources, and user interface design. This subsection provides insights into the potential opportunities and future developments in the field of 3D map visualization in GIS.

2 Traditional 2D Map Visualization

2.1 Overview of Traditional 2D Map Visualization

Traditional 2D map visualization has been the foundation of GIS, providing a visual representation of spatial data on a flat surface. It involves the use of symbols, colors, and other graphical elements to convey information about the spatial features, attributes, and relationships. 2D map visualization has been widely used for spatial analysis, decision making, and communication in various fields such as urban planning, environmental management, transportation, and agriculture. It has proven to be effective in visualizing geographic data, identifying patterns, and making informed decisions.

2.2 Limitations of 2D Map for Spatial Analysis and Decision Making

Despite its widespread use, traditional 2D map visualization has certain limitations that can hinder spatial analysis and decision making. One of the main limitations is the lack of depth perception, which can make it challenging to understand the 3D nature of spatial data. This can result in misinterpretation of spatial relationships and inaccurate analysis. Another limitation is the inability to represent complex spatial features and their interactions in an intuitive manner, such as visualizing the interior of buildings, underground infrastructure, or complex terrains. Additionally, 2D maps can sometimes fail to effectively convey the scale, elevation, and other three-dimensional characteristics of spatial data, which can impact decision making in certain applications.

2.3 Need for More Advanced Visualization Techniques

The limitations of traditional 2D map visualization have led to the development of more advanced visualization techniques, particularly 3D map visualization in GIS. 3D visualization techniques enable the representation of spatial data in a more immersive and intuitive manner, providing a better understanding of the spatial relationships, scale, and elevation. They allow for the visualization of complex spatial features and their interactions, providing a more realistic and holistic view of the data. Furthermore, 3D visualization techniques can enhance spatial analysis and decision making by enabling more accurate measurement, simulation, and prediction of spatial phenomena.

3 Early Attempts at 3D Visualization

3.1 First Attempt at 3D Visualization for GIS

The first attempts at 3D visualization for GIS can be traced back to the 1960s and 1970s when computer graphics technology was in its infancy. Researchers and practitioners started exploring ways to represent geographic data in three dimensions, aiming to provide a more realistic and immersive view of the data. These early attempts involved the use of simple wireframe models, basic shading techniques, and limited interactive capabilities. The focus was primarily on visualizing terrain and topographic features, with limited consideration for other types of spatial data [1].

3.2 Challenges in Generation of 3D Maps

Generating 3D maps in GIS during the early attempts posed several challenges. One of the main challenges was the limited availability of computer graphics technology and computing power, which constrained the complexity and realism of the visualizations. The lack of standardized data formats and interoperability made it difficult to integrate and visualize different types of spatial data in a cohesive manner. The absence of user-friendly interfaces and interactive tools also limited the usability and accessibility of 3D visualization tools. Additionally, the lack of adequate data sources for elevation, texture, and other 3D attributes posed challenges in creating realistic and accurate 3D maps.

3.3 Examples of Early 3D Visualization Tools

Despite the challenges, several pioneering efforts led to the development of early 3D visualization tools for GIS. One of the notable examples is the "SYMAP" system developed in the 1960s by Howard Fisher, which allowed for the creation of simple 3D maps by overlaying elevation data on topographic maps. Another example is the "Geographic Information Visualization and Analysis System" (GIVAS) developed in the 1970s by David Rhind and colleagues, which allowed for the visualization of 3D terrain models and other spatial data. The "SYMAP" and "GIVAS" systems laid the foundation for subsequent advancements in 3D visualization techniques and technologies in GIS.

4 Advancements in 3D Visualization Technology

4.1 Development of Advanced 3D Rendering Engines

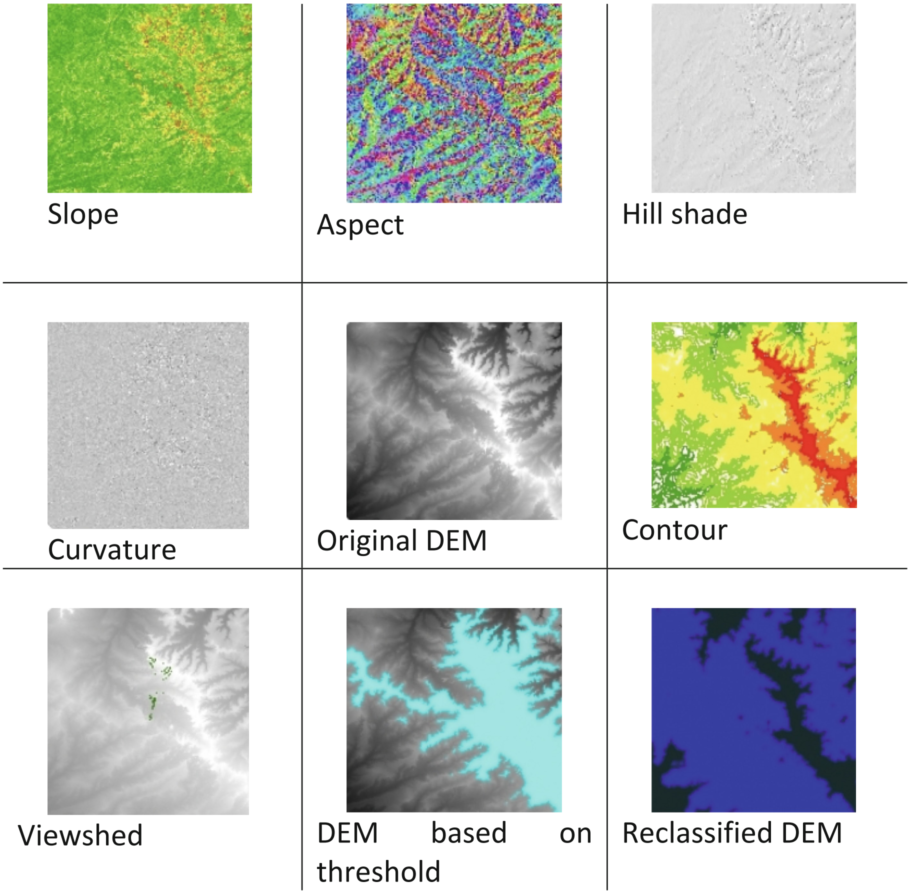
The development of advanced 3D rendering engines has been a significant milestone in the evolution of 3D visualization technologies for GIS. These rendering engines utilize sophisticated algorithms and techniques to generate realistic and visually appealing 3D graphics. One notable example is the "OpenGL" rendering engine, which has been widely used in GIS applications for rendering 3D models and visualizing terrain data. Another example is the "Unity" game engine, which has gained popularity in GIS for its real-time rendering capabilities and support for advanced visual effects. These advanced 3D rendering engines have enabled the creation of high-quality and interactive 3D visualizations in GIS, allowing for more effective communication and decision-making.

4.2 Integration of GIS Data with 3D Models

The integration of GIS data with 3D models has been a significant advancement in 3D visualization technologies for GIS. This integration allows for the seamless overlay of GIS data, such as satellite imagery, aerial photographs, and vector data, on top of 3D models, enabling a more comprehensive and contextual understanding of the spatial relationships [2]. This integration has been facilitated through the use of Geographic Information System Markup Language (GISML), which provides a standardized format for encoding and exchanging GIS data in 3D visualizations. The integration of GIS data with 3D models has opened up new possibilities for advanced spatial analysis and decision-making in GIS, allowing for more accurate and insightful visualizations.

4.3 Terrain Visualization Techniques for 3D

Digital Elevation Models (DEM): DEMs are raster representations of terrain elevations that are widely used in 3D GIS. They can be derived from various sources, such as LiDAR, photogrammetry, or satellite imagery [3]. The process involves data acquisition, pre-processing (e.g., filtering, interpolation), and post-processing (e.g., visualization, analysis). DEMs are commonly used for terrain analysis, hydrological modeling, and visualization in 3D GIS [4] (Fig. 1).



Slope

Aspect

Hill shade

Curvature

Original DEM

Contour

Viewshed

DEM based on threshold

Reclassified DEM

Fig. 1. Analysis of DEM

Triangulated Irregular Networks (TIN): TINs represent terrain as a network of non-overlapping triangles, defined by their vertices and associated elevations. TINs are preferred for their ability to accurately capture complex terrain features, such as cliffs or overhangs. The process involves data acquisition, triangulation, and post-processing (e.g., visualization, analysis). TINs are commonly used for terrain modeling in applications like urban planning, flood modeling, and slope stability analysis.

The following figure is an illustration of how a triangulated irregular network dataset is created using a subset of the nodes from source triangulated irregular network. We can see as an output, thinning of the oversampled data from the input (Fig. 2).

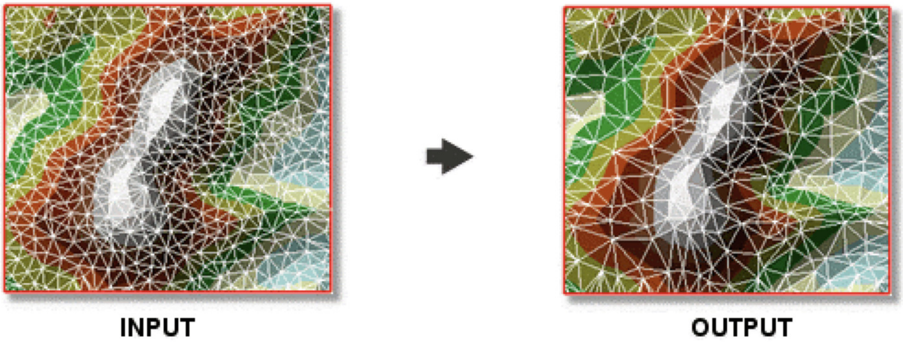


Fig. 2. Generation of TIN

Interpolation Techniques: Interpolation methods, such as Inverse distance weighting (IDW), kriging, spline, and nearest neighbour, estimate terrain elevations at un-sampled locations based on known elevation values. These techniques involve mathematical equations that use nearby elevation values to estimate elevations at un-sampled locations. The process involves data acquisition, selection of interpolation method, parameterization, interpolation, and post-processing (e.g., visualization, analysis). Interpolation is widely used for generating smooth terrain surfaces from sparse elevation data, and is used in applications like land use planning, viewshed analysis, and habitat modeling.

Photogrammetry: Photogrammetry is a technique that uses overlapping aerial or satellite imagery to extract terrain elevations. It involves capturing multiple images from different viewpoints and using geometric and radiometric properties of the images to estimate terrain elevations. Photogrammetry requires complex algorithms, such as bundle adjustment, triangulation, and orthorectification, to accurately estimate elevations [5]. The process involves image acquisition, image processing, feature extraction, and terrain elevation estimation. Photogrammetry is commonly used for terrain mapping in applications like topographic mapping, forest inventory, and coastal zone management. The Fig. 3 is an example of an 3d structure of a port being generated through photogrammetry.

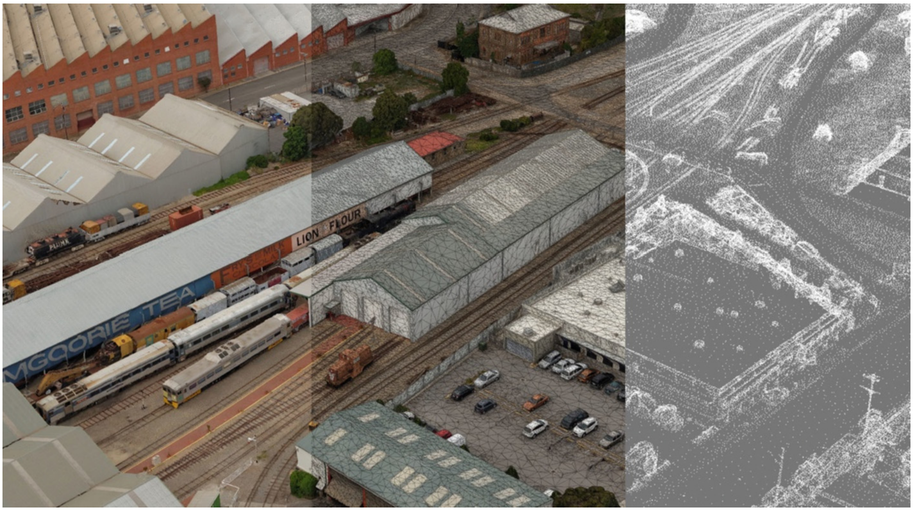


Fig. 3. 3D city model (port Adelaide), being generated through photogrammetry

4.4 Examples and Comparison of Modern 3D Visualization Tools

There are several modern 3D visualization tools that have emerged with advancements in 3D visualization technologies for GIS. These tools provide various features and functionalities for creating and interacting with 3D visualizations. For example, "ArcGIS Pro" by Esri is a popular GIS software that provides advanced 3D visualization capabilities, including the ability to create realistic 3D scenes, integrate GIS data with 3D models, and perform advanced spatial analysis in a 3D environment. "Google Earth" is another widely used tool that allows for the exploration of 3D maps and satellite imagery in a virtual globe environment. "Cesium" is an open-source JavaScript library that enables the creation of web-based 3D visualizations with high interactivity and customization [8]. These modern 3D visualization tools provide a wide range of visualization options, including tabular, charts, and graphs, for presenting and analyzing spatial data in a visually compelling manner (Fig. 4).

The generated 3D scatter plot visually compares the performance, user interface, and data analysis aspects of different GIS software, including ArcGIS Pro, QGIS 3, ArcGIS Desktop, Hexagon Geomedia, and MapInfo Professional. The X-axis represents performance, the Y-axis represents user interface, and the Z-axis represents data analysis. Each software is represented by a marker in the plot, with its position on the three axes indicating its respective ranking in terms of performance, user interface, and data analysis. The color of the marker is determined by a color palette, and the legend in the upper left corner of the plot provides the mapping of colors to the respective software. The plot provides a visual comparison of these parameters for the different GIS software, allowing for a quick understanding of how they rank against each other in terms of performance, user interface, and data analysis.

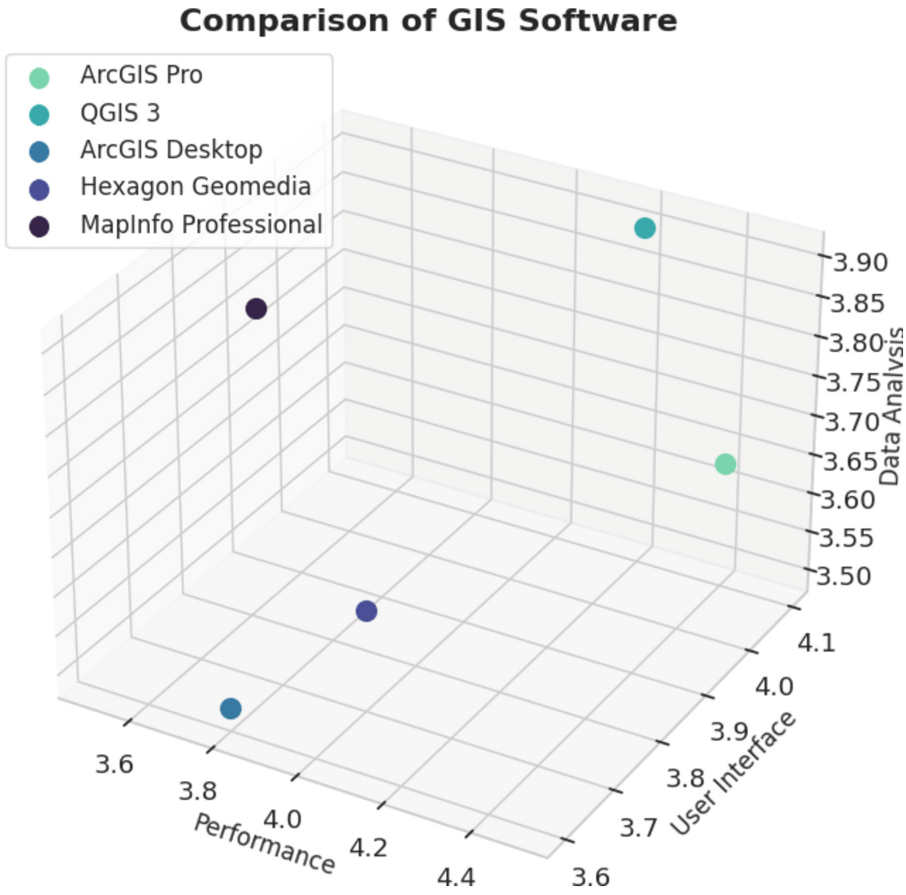


Fig. 4. Comparison of GIS software through 3D scatter plot

5 Applications of 3D Visualization in GIS

5.1 Urban Planning and Architecture

3D visualization has revolutionized urban planning and architecture by providing an immersive and interactive way to visualize complex urban landscapes. It allows urban planners and architects to create realistic 3D models of cities, buildings, and infrastructure, which can be used for various purposes. For instance, 3D visualization enables the assessment of the impact of new developments on the urban environment, the simulation of different scenarios to optimize city planning, and the visualization of future urban designs to engage stakeholders and the public. Moreover, 3D visualization facilitates urban design and architecture by allowing architects to visualize and manipulate building designs in a virtual environment, leading to more informed decisions and improved designs.

5.2 Natural Resource Management

3D visualization has transformed the field of natural resource management by providing a powerful tool for visualizing and analyzing complex spatial data related to natural resources. For instance, in forestry, 3D visualization allows the creation of realistic models of forest landscapes, enabling the assessment of tree height, density, and species distribution for better forest management. In geology, 3D visualization helps in the exploration and mapping of mineral resources by visualizing subsurface geology and identifying potential resource-rich areas. Additionally, 3D visualization facilitates the visualization and monitoring of environmental changes, such as deforestation, land degradation, and habitat fragmentation, aiding in the conservation and sustainable management of natural resources.

5.3 Emergency Response and Disaster Management

3D visualization plays a crucial role in emergency response and disaster management by providing situational awareness and decision support tools for response teams. During disasters, 3D visualization allows the visualization of real-time data, such as weather patterns, flood extent, or fire spread, facilitating the assessment of the situation and the planning of response strategies. It also aids in the communication of critical information to decision-makers, emergency responders, and the public, leading to more effective and coordinated responses. Furthermore, 3D visualization supports the pre-disaster planning and preparedness efforts by visualizing vulnerable areas, evacuation routes, and infrastructure networks, enabling better decision-making and resource allocation.

5.4 Military and Defense Applications

3D visualization has significant applications in the military and defense sectors, where it aids in mission planning, training, and decision-making. For instance, in military operations, 3D visualization allows the visualization of terrain, infrastructure, and potential threats, facilitating the planning of strategic and tactical operations. It also supports military training by providing realistic virtual environments for simulations and exercises, leading to improved preparedness and decision-making skills. Additionally, 3D visualization enables the visualization of intelligence, surveillance, and reconnaissance (ISR) data, aiding in situational awareness and decision-making in defense operations.

Here are some examples where GIS has been reported to have contributed to military and defense operations:

Battlefield Situational Awareness: GIS technology is used to create maps and visualize real-time data, providing military personnel with critical situational awareness information such as troop movements, terrain analysis, and enemy locations. This helps in making informed decisions and planning military operations effectively.

Intelligence, Surveillance, and Reconnaissance (ISR): GIS is used to gather, analyze, and visualize spatial data from various sources, such as satellite imagery, aerial photography, and ground-based sensors, to support military intelligence and surveillance efforts. This helps in monitoring and analyzing enemy activities, identifying potential threats, and planning countermeasures.

Logistics and Supply Chain Management: GIS is used to optimize the movement of personnel, equipment, and supplies by analyzing geographic data such as transportation routes, supply depots, and storage facilities. This helps in efficient allocation of resources and coordination of logistics operations, especially in remote or hostile environments.

Crisis Response and Disaster Management: GIS is used to support disaster management and humanitarian relief efforts by providing real-time information on affected areas, infrastructure damage, evacuation routes, and distribution of resources. This helps in coordinating emergency response efforts and allocating resources effectively.

6 Challenges and Future Directions

6.1 Challenges Faced by Developers and Researchers in Creating Accurate and Realistic 3D Models

Accuracy of Data: Spatial data used for creating 3D models, such as elevation data, satellite imagery, and 3D building models, may have inherent errors and inaccuracies that can affect the quality of the 3D models [6]. Ensuring accurate and precise data acquisition is critical for creating realistic 3D representations of the real world in GIS.

Complexity of 3D Modeling Techniques: 3D modeling involves complex algorithms and computations to generate 3D representations from 2D spatial data. Developing and implementing accurate 3D modeling algorithms can be challenging, requiring expertise in computer graphics, mathematics, and spatial analysis. Furthermore, the scalability and performance of 3D modeling techniques can be a challenge when dealing with large and complex geographic datasets.

Diversity and Heterogeneity of Data Sources: Different data sources in GIS may have varying levels of detail, accuracy, and format, making it challenging to create seamless and realistic 3D representations. Ensuring consistency and compatibility among different data sources is crucial for creating accurate and realistic 3D models in GIS.

In summary, the challenges in creating accurate and realistic 3D models in GIS include data accuracy, complexity of 3D modeling techniques, and diversity and heterogeneity of data sources. Overcoming these challenges requires advanced data acquisition and processing techniques, as well as expertise in computer graphics, mathematics, and spatial analysis.

6.2 Need for Better Data Acquisition and Processing Techniques

To address the challenges in creating accurate and realistic 3D models, there is a need for better data acquisition and processing techniques in GIS. Accurate and high-resolution data acquisition methods, such as LiDAR (Light Detection and Ranging) and photogrammetry, can provide more precise and detailed elevation data for creating realistic 3D models. These data acquisition techniques can capture fine-grained details of the terrain, vegetation, and buildings, enabling more accurate and realistic 3D representations.

In addition to data acquisition, data processing techniques play a crucial role in creating accurate and realistic 3D models. Advanced data processing techniques, such as feature extraction, data fusion, and data integration, can help in integrating diverse and heterogeneous data sources to create seamless and realistic 3D representations. These techniques can also address the challenges of scalability and performance by optimizing the processing algorithms for large and complex geographic datasets.

6.3 Potential for Virtual and Augmented Reality in GIS

Virtual and augmented reality (VR/AR) technologies have the potential to revolutionize the way we interact with GIS data in 3D visualizations [7]. VR allows users to immerse themselves in a virtual environment and interact with 3D models in a more natural and intuitive way. AR, on the other hand, overlays virtual content on the real world, allowing users to visualize and interact with GIS data in real-time and real-world context.

The use of VR/AR in GIS can enhance the user experience and enable more effective spatial analysis and decision-making. For example, military and defense applications can benefit from VR/AR by providing realistic and immersive training environments for soldiers, visualizing battlefield situational awareness, and planning military [9].

7 Future Scope

7.1 Augmented Reality/Virtual Reality (AR/VR) Integration

Use-case: Imagine a team of urban planners tasked with designing a new city district. They need to analyse the existing terrain, consider various infrastructure options, and ensure the optimal use of available space. Traditionally, they would rely on 2D maps and blueprints to visualize the project. However, with the integration of augmented reality (AR) in their GIS platform, the planners now have access to a more immersive experience.

Using AR glasses and mobile devices, the planners can walk through the proposed district while visualizing 3D terrain models overlaid with real-time data. They can virtually see buildings, roads, and parks on the terrain, allowing them to assess the impact of their design choices in a realistic context. For instance, they can visualize the shadows cast by buildings at different times of the day, evaluate potential flood risk areas, and even simulate how the district would look during extreme weather conditions. This interactive AR integration empowers planners to make more informed decisions and engage with stakeholders effectively.

7.2 Real-Time Data Integration

Use case: During a wildfire outbreak, emergency response teams are challenged with rapidly changing terrain conditions and spreading fire patterns. With real-time data integration in their GIS system, the response teams can access up-to-date information from satellite imagery, weather sensors, and drones.

Using a tablet-based GIS application, the teams can visualize the current fire front in real-time on a 3D terrain model. The GIS platform automatically updates the terrain model with live satellite data, showing the precise location of the fire front and potential areas of concern. Additionally, the system overlays the terrain with temperature, wind direction, and humidity data, enabling the teams to predict the fire's future behavior more accurately.

By utilizing real-time data integration, the emergency response teams can efficiently allocate resources, plan evacuation routes, and coordinate firefighting efforts. This capability saves crucial time and helps in mitigating the impact of wildfires on communities and the environment.

7.3 AI-Driven Terrain Analysis

Use case: An environmental conservation group is monitoring the habitat of endangered species in a vast national park. Traditional methods of manually identifying and tracking habitats are time-consuming and resource-intensive. To address this challenge, they adopt an AI-driven terrain analysis approach in their GIS platform.

Using machine learning algorithms, the GIS system automatically analyses satellite imagery and LiDAR data to identify distinct terrain features relevant to the species' habitat [12]. The AI model can recognize specific vegetation patterns, water bodies, and geological formations that are critical to the species' survival. As a result, the conservationists can quickly identify potential areas of interest, track changes in habitat over time, and prioritize conservation efforts efficiently.

The AI-driven terrain analysis not only enhances the accuracy of habitat identification but also enables the conservation group to focus their limited resources on protecting the most crucial areas for endangered species.

7.4 Collaborative 3D Visualization

Use case: A team of urban designers, architects, and landscape planners is collaborating on a large-scale urban redevelopment project. Each team member brings expertise in their respective domains, and effective collaboration is essential for successful outcomes.

Using a cloud-based collaborative 3D visualization platform, the team can work together in real-time, regardless of their physical locations. Each member can access the 3D terrain model and make modifications, such as adding buildings, parks, or roads, while the changes are instantly visible to others. Furthermore, they can leave comments, annotations, and suggestions directly on the terrain model, fostering seamless communication and idea sharing.

In a virtual meeting, the team gathers to discuss the proposed changes while navigating the 3D terrain collaboratively. This immersive experience allows them to understand the spatial relationships better and make informed decisions collectively. The collaborative 3D visualization platform streamlines the design process, reduces coordination efforts, and facilitates a more cohesive approach to urban planning.

7.5 Environmental Monitoring and Climate Change Visualization

Use case: A team of environmental researchers is studying the impact of climate change on glaciers in a remote mountain range. To visualize the changes over time, they employ an advanced GIS platform that combines historical satellite imagery with present-day data.

The GIS system generates a 3D terrain model of the glacier using high-fidelity satellite mapping. By comparing this model with historical data, the researchers can observe the glacier's retreat and measure its changing volume. Additionally, they overlay temperature and precipitation data on the terrain to understand the climate conditions influencing glacier behaviour.

Through animated visualization, the researchers observe the glacier's progression over several decades, highlighting the alarming rate of ice loss due to climate change. This powerful visual representation aids in raising awareness among policymakers and the public about the urgency of climate action.

7.6 Mobile 3D Visualization Platforms

Use case: A team of geologists is conducting fieldwork in a remote and rugged terrain, surveying geological formations and collecting rock samples. In the past, they had to rely on traditional handheld GPS devices and paper maps for navigation, making it challenging to correlate their findings with the larger terrain context [10].

With the adoption of mobile-based 3D visualization platforms, the geologists can now access a portable GIS system on their tablets or smartphones. The platform offers real-time 3D terrain visualization, allowing them to identify geological features more accurately and understand their spatial relationships [11].

During their field surveys, the geologists can quickly validate their observations by visualizing their collected data on the 3D terrain model. This real-time feedback enhances the quality of their findings and ensures the integration of their data into the larger GIS database seamlessly.

References

1. Goodchild, M.F., Quattrochi, D.A.: Scale in Remote Sensing and GIS. CRC Lewis, Boca Raton (1997)
2. Panigrahi, N., Panigrahi Sankalp, S.: Processing data acquired by a drone using a GIS: designing a size-, weight-, and power-constrained system. IEEE Consum. Electron. Mag. **7**(2), 50–54 (2018). https://doi.org/10.1109/mce.2017.2714718
3. Narayan, P.: Geographical Information Science. The University Press, Hyderabad (2009). ISBN (13) 978-1-4398-1004
4. Ruzinoor, C.M., Shariff, A.R.M., Pradhan, B., Rodzi Ahmad, M., Rahim, M.S.M.: A review on 3D terrain visualization of GIS data: techniques and software. Geo-spat. Inf. Sci. **15**(2), 105–115 (2012). https://doi.org/10.1080/10095020.2012.714101
5. Bolstad, P., Stowe, T.: An evaluation of DEM accuracy: elevation, slope, and aspect. Photogram. Eng. Remote Sens. **60**, 1327–1332 (1994)

6. Palmer, D., Koumpli, E., Cole, I., Gottschalg, R., Betts, T.: A GIS-Based method for identification of wide area rooftop suitability for minimum size PV systems using LiDAR data and photogrammetry. Energies **11**(12), 3506 (2018). https://doi.org/10.3390/en11123506
7. Zhou, C., et al.: COVID-19: challenges to GIS with Big Data. Geogr. Sustain. **1**(1), 77–87 (2020). https://doi.org/10.1016/j.geosus.2020.03.005
8. Geospatial and photogrammetry: When the mapping world and the gaming world collide. www.linkedin.com. https://www.linkedin.com/pulse/geospatial-photogrammetry-when-mapping-world-gaming-collide-marre/. Accessed 9 Apr 2023
9. osgEarth: Main Page. updraft.github.io. https://updraft.github.io/osgearth-doc/html/index.html. Accessed 9 Apr 2023
10. Li, X., Lv, Z., Hu, J., Zhang, B., Shi, L., Feng, S.: XEarth: a 3D GIS platform for managing massive city information. In: 2015 IEEE International Conference on Computational Intelligence and Virtual Environments for Measurement Systems and Applications (CIVEMSA) (2015). https://doi.org/10.1109/civemsa.2015.7158625
11. Xiong, L., Li, S., Tang, G., Strobl, J.: Geomorphometry and terrain analysis: data, methods, platforms and applications. Earth Sci. Rev. **233**, 104191 (2022). https://doi.org/10.1016/j.earscirev.2022.104191
12. Ganesh, B., Vincent, S., Pathan, S., Raquel, S.: Integration of GIS and machine learning techniques for mapping the landslide-prone areas in the state of Goa, India. J. Indian Soc. Remote Sens. **51**, 1479–1491 (2023). https://doi.org/10.1007/s12524-023-01707-y

Generic Medicine Recommender System with Incorporated User Feedback

Sneh Shah[3], Varsha Naik[3], Debajyoti Mukhopadhyay[1],
and Swapnoneel Roy[2](✉)

[1] WIDiCoReL Research Lab, Mumbai, India
[2] University of North Florida, Jacksonville, FL 32246, USA
s.roy@unf.edu
[3] Dr. Vishwanath Karad MIT World Peace University, Pune, India

Abstract. This paper presents the implementation of a Generic Medicine Recommender System (GMRS) that incorporates user feedback as a solution to streamline the selection process of appropriate generic medication and improve overall quality of healthcare. The study evaluates the suggestions given by the Generic Medicine Recommender System (GMRS), enhance the suggestions based on user input, and comprehend the influence of these suggestions on patient outcomes following the usage of generic medications. The results imply that the GMRS not only has the potential to enhance patient outcomes but can also give important information about the efficacy of various generic medications. The study also emphasizes how critical it is to incorporate user input into system recommendations in order to maximize performance and the system's effect on healthcare expenses. Recommending generic alternatives to costly prescribed medicines is significant because in addition to ensuring the provision of more broadly accessible drugs for treatment, it assists patients in saving money on their prescription pharmaceuticals. Generic medications have the same amounts of active ingredients as branded drugs. As a result, when it comes to treating sickness, generic medications are often as effective as branded medications.

Keywords: Recommendation Systems · Generic Medicines · User Feedback

1 Introduction

The use of generic medicines has been on the rise in recent years, with many patients and healthcare providers recognizing their effectiveness and cost-saving benefits. The Indian generic medicine market, which was valued at USD 24.53 billion in 2022, is anticipated to expand at a consistent compound annual growth rate (CAGR) of 6.97% over the projection period. According to the Economic Survey 2022–23, which was published on January 31, 2023, India's domestic pharmaceutical industry is projected to reach USD 130 billion by 2030 and the

Published by Springer Nature Switzerland AG 2024
D. Puthal et al. (Eds.): IFIPIoT 2023, IFIP AICT 684, pp. 64–73, 2024.
https://doi.org/10.1007/978-3-031-45882-8_5

pharma market has maintained its growing pace following the Covid-19 pandemic. The problem is that, despite the fact that there are generic alternatives that work just as well, patients prefer to spend more money on brand-name medications. These alternatives are not frequently given by doctors, but if patients were made aware of them, they might have a substantial socioeconomic impact. Any generic pharmaceutical recommender system's success depends heavily on user feedback. As patients feel more invested in their healthcare decisions when they have a part in the suggestion process, user feedback can aid in fostering trust and engagement with the system. A project that would recommend generic medications with the same active ingredients as brand-name medications is being presented as a solution to this problem. By raising knowledge of less expensive options, this method would help both patients and doctors.

1.1 Our Contributions

The implementation of a Generic Medicine Recommender System (GMRS) that incorporates user feedback is discussed in this study as a way to speed up the process of choosing the best generic medications and enhance healthcare quality in general. The study assesses the recommendations made by the Generic Medicine Recommender System (GMRS), improves the recommendations based on user feedback, and determines how these recommendations affect patient outcomes after taking generic pharmaceuticals. According to the findings, the GMRS not only has the potential to improve patient outcomes, but it can also provide crucial details regarding the effectiveness of various generic drugs. The study also highlights how crucial it is to take user feedback into account when formulating system suggestions in order to enhance performance and the system's impact on healthcare costs.

2 Related Work

Fulwani et al. [8] proposed a GMRS based on collaborative filtering and Cloud Vision API that suggested generic alternatives to prescribed medicines by matching their active ingredients, while also providing information about potential side effects, dosage, and cost. Their goal was to improve patient access to cost-effective medicine options and increase the awareness about medicine choices. In addition to their proposed model, we are incorporating user feedback which helps in improving the recommendations and overall a better user experience. Peska [16] proposed several context-related features and evaluated their impact on purchase prediction. The results show that incorporating context improves the performance of prediction models. Furthermore, by using purchase probability as a proxy for user engagement, the quality of recommendations improved in terms of nDCG and recalltop-k. However, the study did not investigate the individual effects of each contextual feature and the possibility of combining purchase probabilities from different methods, which are suggested as future research directions. Kushwaha et al. [14] propose a drug recommendation system that combines semantic web technology and data mining algorithms to extract semantic data and individualize treatment based on a patient's attributes. The system also takes into account drugs that the patient has taken before and potential interactions. The results demonstrate that the proposed system is able to improve the overall treatment outcomes by providing personalized treatment recommendations. Abhishek et al. [1] presents a medicine recommender system that uses a machine learning approach to suggest appropriate medications for patients. The model uses content-based, collaborative, or hybrid approaches to recommend drugs based on the ratings of users' experiences with them. The study uses a 10-fold cross-validation to evaluate the topN recommender algorithm by analyzing five randomly picked items. Ochoa et al. [15] discusses the use of medical recommender systems that utilize continuous-valued logic and multi-criteria decision operators, and are implemented using interpretative neural networks. The authors applied a method for data synthetization, resulting in an error of 1% for all relevant parameters and LONN models with an accuracy of 75%, though less accurate than conventional deep-learning models by 8%, but compensated by the transparency and safety due to freezing of training parameters making them less vulnerable to adversarial attacks. Bhoi et al. [3] describes an end-to-end system called PREMIER that uses information from past and current visits, along with drug information, to make accurate recommendations for medical prescriptions, with a focus on minimizing adverse drug interactions. Fang et al. [7] proposes a novel explicit feedback recommendation method using user-generated content (UGC) to solve the sparsity problem of recommendation systems. The method uses CNN models and textual semantic analysis techniques to identify product features and customer needs from UGC, and an attention mechanism and antonym mechanism to measure the user-product fit degree. Goyal et al. [11] presented a universal medicine recommender system framework that applies data mining technologies to the medical diagnosis. Experiments are done to evaluate the models and it is found that SVM is selected for the medicine recommendation model for its high accuracy, good efficiency and scalability. The system also includes a mistaken-check mechanism for safety and quality assurance. Future work includes building a custom recommendation model and using Map Reduce parallel technologies to improve the system's ability to process big diagnosis data. Granda et al. [12] presented a recommender system (RS) for suggesting medications suitable for patients with diabetes. The system uses user metadata and clustering techniques to alleviate the cold-start problem, resulting in groups of patients with similar characteristics and providing drug recommendations for patients in the same cluster and offers a new method to support health care personnel in medical care and management of patients with diabetes and can be further improved by using more drug information or combining with other collaborative filtering approaches. Bhimavarapu et al. [2] proposed a deep learning-based drug recommendation system that utilizes a loss function to improve fairness and accuracy. The system takes lab test results from patients with co-morbidities and uses statistical analysis to adjust the threshold value, balancing fairness and accuracy. The results of the proposed system showed an accuracy of 98.5%, indicating that the ANN model is an accepted model for drug recommendation systems.

3 Methodology

The proposed methodology, at a higher level, contains the depicted steps (Fig. 1).

3.1 Data Acquisition

The dataset contains the following 6 fields:

1. DrugName: The drug name (Mirtazapine).
2. Condition: The condition which the drug treats (Depression).
3. Review: The user review *"I've tried a few antidepressants over the years (citalopram, fluoxetine, amitriptyline), but none of those helped with my depression, insomnia &amp; anxiety. My doctor suggested and changed me onto 45mg mirtazapine and this medicine has saved my life."*
4. Rating: The rating for the drug based on the effect (10).
5. UsefulCount: The count of users who found the drug useful (22).
6. Generic Alternative: The alternative generic medicines (Remeron, Remergil).

The project is built upon two different datasets:

1. The first dataset (Fig. 2) is gathered by web scraping.
2. The second dataset (Fig. 3) is sampled from an open source dataset.

3.2 Data Visualization

In addition to developing a pharmaceutical recommendation system, we applied visualisation tools to help us comprehend the data and effectively convey our findings. To depict the data, we employed a range of graphs, including scatter plots, bar charts, and histograms. These plots clearly showed the distribution of ratings for each medicine, the frequency of each condition in the dataset, and the relationship between ratings and usefulCount for each drug. We were able to spot patterns and trends in the data as well as acquire understanding of the traits of the medications in the dataset thanks to the visualization. Finally, visualisation helped us grasp the data more efficiently and successfully communicate our findings.

3.3 Collaborative Filtering

To analyze user historical behavior data, discover the relationship between users' or objects' preferences, and subsequently provide recommendations, a standard collaborative filtering method is used. The algorithm can be broken down into four steps: data description, k-nearest neighbor finding, rating prediction, and recommendation generation. The essential premise of the collaborative filtering approach is that if two people A and B have the same view on a subject, A is more likely to share B's perspective on a different subject than would be the case with a randomly selected person.

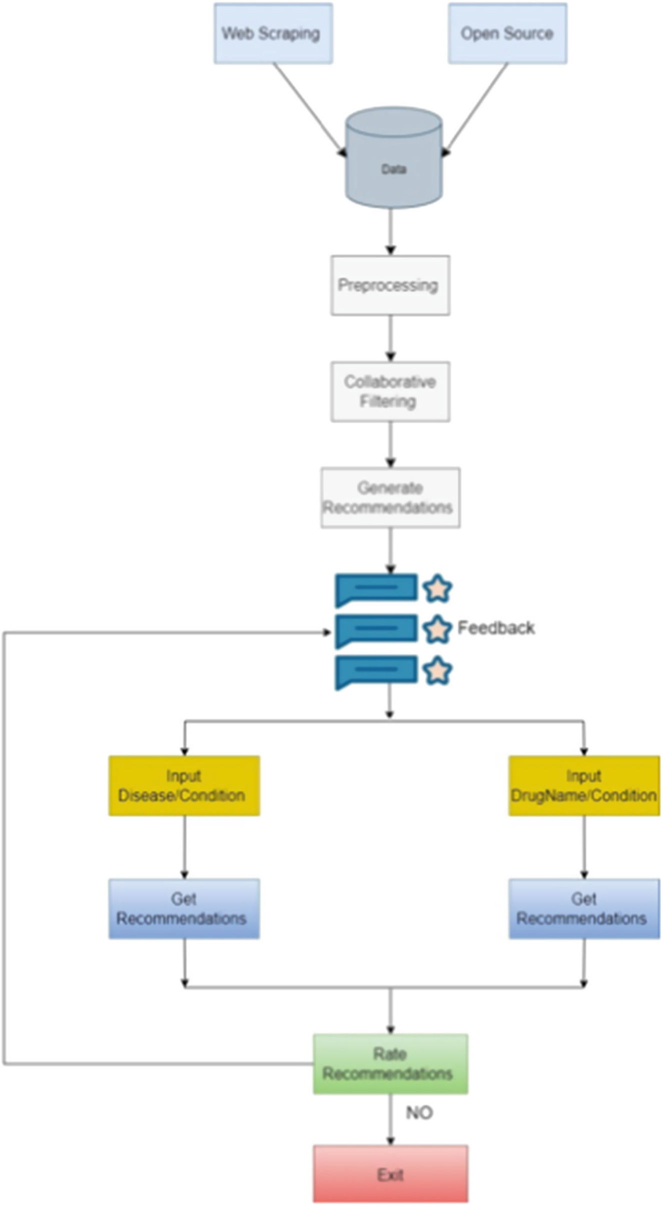


Fig. 1. Proposed Methodology Flowchart with Incorporated User Feedback

The process of computing similarity is the most crucial part of the entire algorithm. There are various ways to calculate similarities, including the Pearson correlation co- efficient, cosine-based similarity, and adjusted cosine similarity

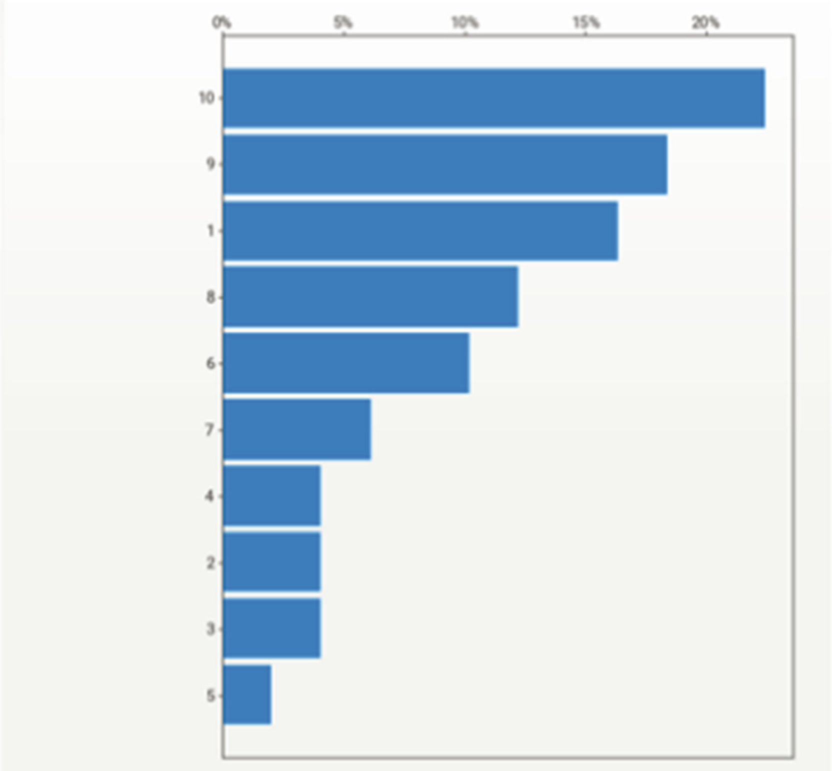


Fig. 2. Distribution of ratings provided by the user

out of which we have used cosine-based similarity to generate similarities between a particular medicine and all the other medicines.

$$sim(a, b) = cos(\boldsymbol{a}, \boldsymbol{b}) = \frac{\boldsymbol{a} \cdot \boldsymbol{b}}{\parallel \boldsymbol{a} \parallel \times \parallel \boldsymbol{b} \parallel} \tag{1}$$

Where $sim(a, b)$ is the similarity between a and b.

3.4 Vector Embeddings

Word2vec. With the help of a huge text corpus, the word2vec technique employs a neural network model to learn word associations. Once trained, a model like this can identify terms that are similar or suggest new words to complete a sentence. As the name suggests, word2vec uses a specific set of numbers called a vector to represent each unique word. Given that the vectors were properly selected to capture the semantic and syntactic characteristics of words, the degree of semantic similarity between the words represented by those vectors may be determined using a straightforward mathematical function (cosine similarity). With the exception of having no linear hid- den layer, the Continuous

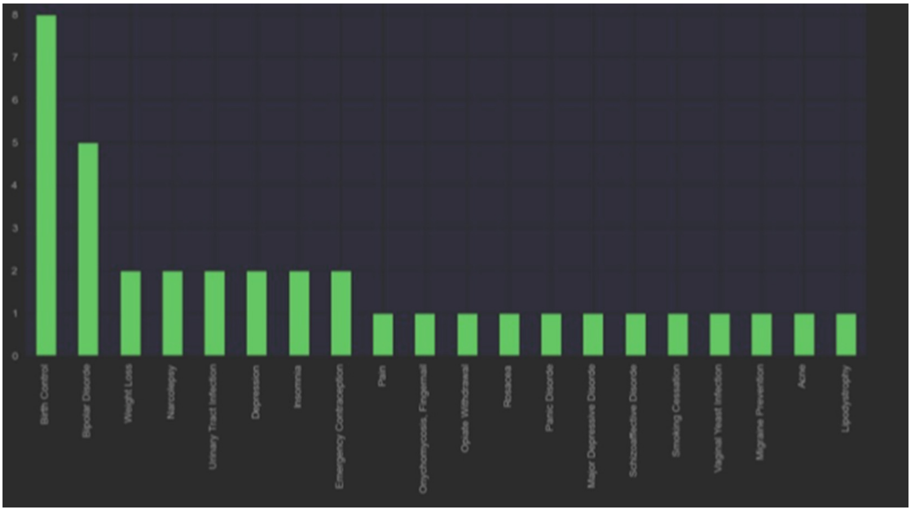


Fig. 3. Number of drugs per condition in the dataset (Top 20 drugs)

bag of words model (CBOW) model is derived from the NNLM model. When previous $N/2$ history words and future $N/2$ words are provided, the CBOW model's goal function is to predict the middle word. The $N = 8$ value yields the best outcome. Word vectors of N context words are simply averaged in the projection layer. Because the word's position has no bearing on the word vector of the middle word, the nickname *Bag of Words* has been coined. Here, we have used Word2vec to create embedding for the user review feature and incorporated them to give the users more enhanced recommendations.

FastText. In contrast to Word2vec, which treats each word as the smallest unit for which a vector representation must be found, FastText assumes that words are formed by n-grams of characters. For instance, the word sunny is made up of [sun, sunn, sunny], [sunny, unny, nny], etc., with n ranging from 1 to the word's length. Compared to word2vec this new word representation from fastText offers many advantages. It can provide vector representations for words that are not in dictionaries (OOV words), as these words can also be divided into character n-grams. Word2vec falls short of offering any vector representations for words not found in dictionaries. For instance, gensim might provide either one of the following two results for a term like *stupedofantabulouslyfantastic*, which may not have been in any corpus: a) a zero vector or b) a random vector with a small magnitude. But by splitting the aforementioned word into smaller pieces and using the vectors for those pieces to form a final vector for the word, FastText can generate vectors that are better than those produced at random. The resulting vector in this scenario might resemble the vectors of wonderful and fantabulous more closely. We chose FastText as it provides significantly better embedding since it works on a more granular level with character n-grams as compared to Word2vec.

3.5 Explicit User Feedback

In order to improve the generic drug suggestion process, explicit user feedback is essential. We learned a lot about user preferences and experiences with various medications by directly requesting user feedback through ratings and reviews. Identifying particular medications that users consistently evaluate highly is one method that explicit user feedback was used to improve recommendations. By examining this input over a long period of time, we can modify our algorithms for recommending the generic medicines in a way that gives priority to these highly rated medications and gives customers recommendations that are more tailored and useful. On the other hand, if users repeatedly rate a particular medication as ineffective or report suffering unfavourable side effects, this data can be utilised to modify the recommendation algorithm and stop prescribing that medication in the future.

4 Results

High user ratings and comparisons to the reference drugs supported the recommendation model's findings that it produced accurate and pertinent recommendations for users. The model's overall effectiveness was increased by its capacity to produce personalized suggestions based on the patient's condition and personal drug preferences. The validation's use of both subjective and objective measurements showed that the model's output was stable and reliable. The outcomes offers convincing proof of the recommendation model's value in assisting consumers in selecting the optimal generic medications.

5 Conclusion

The use of a Generic Medicine Recommender System (GMRS) has the potential to completely change how appropriate generic medications are chosen, raise patient care standards, and lower healthcare expenditures. The GMRS's inclusion of user feedback offers insightful data on the efficacy of various generic medications that doctors can utilize to guide deliberations. Overall, the results point to the GMRS as having a favorable effect on patient outcomes, making it a viable option for guaranteeing more access to medications for medical treatment and supporting patients in lowering their costs for prescription medications.

6 Future Directions

Future studies should involve making the GMRS available to a larger number of audience and evaluate the effectiveness in different settings. For example, to help healthcare providers and pharmacists in recommending generic alternatives to patients, the system could be implemented in hospitals, clinics and pharmacies. Moreover, the future studies should also focus on enhancing the user feedback mechanism to improve the recommendations. Future studies could also look into how the GMRS may affect patients' adherence to their prescribed medications as it may have significant effects on patient outcomes and healthcare spending. This may entail determining if individuals are more likely to adhere to their treatment schedule when given generic drugs that the system recommends. Also of interests would be to assess such systems with regards security (e.g. [9,10,13,17–20]) and improvements in the sustainability (e.g. energy consumption [4–6,21,22]) of such recommender systems.

Acknowledgement. The research has been supported in part by Fidelity National Financial Distinguished Professorship in CIS grant of S. Roy, 0583-5504-51.

References

1. Abhishek, A., Bindal, A.K., Yadav, D.: Medicine recommender system: a machine learning approach. In: AIP Conference Proceedings, vol. 2576. AIP Publishing (2022)
2. Bhimavarapu, U., Chintalapudi, N., Battineni, G.: A fair and safe usage drug recommendation system in medical emergencies by a stacked ANN. Algorithms **15**(6), 186 (2022)
3. Bhoi, S., Lee, M.L., Hsu, W., Fang, H.S.A., Tan, N.C.: Personalizing medication recommendation with a graph-based approach. ACM Trans. Inf. Syst. (TOIS) **40**(3), 1–23 (2021)
4. Castellon, C., Roy, S., Kreidl, P., Dutta, A., Bölöni, L.: Energy efficient Merkle trees for blockchains. In: 2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp. 1093–1099. IEEE (2021)
5. Castellon, C.E., Roy, S., Kreidl, O.P., Dutta, A., Bölöni, L.: Towards an energy-efficient hash-based message authentication code (HMAC). In: 2022 IEEE 13th International Green and Sustainable Computing Conference (IGSC), pp. 1–7. IEEE (2022)
6. Escobar, C.C., Roy, S., Kreidl, O.P., Dutta, A., Bölöni, L.: Toward a green blockchain: engineering Merkle tree and proof of work for energy optimization. IEEE Trans. Netw. Serv. Manage. **19**(4), 3847–3857 (2022)
7. Fang, B., Hu, E., Shen, J., Zhang, J., Chen, Y.: Implicit feedback recommendation method based on user-generated content. Sci. Program. **2021**, 1–15 (2021)
8. Fulwani, S., Nagdev, R., Megnani, N., Bhatia, M., Giri, N.: Generic medicine recommender system. IJCRT **6**, 880–883 (2018). https://ijcrt.org/papers/IJCRT1803021.pdf
9. Garrett, K., Talluri, S.R., Roy, S.: On vulnerability analysis of several password authentication protocols. Innov. Syst. Softw. Eng. **11**(3), 167–176 (2015). https://doi.org/10.1007/s11334-015-0250-x
10. Gouge, J., Seetharam, A., Roy, S.: On the scalability and effectiveness of a cache pollution based DoS attack in information centric networks. In: 2016 International Conference on Computing, Networking and Communications (ICNC), pp. 1–5. IEEE (2016)

11. Goyal, V.A., Parmar, D.J., Joshi, N.I., Champanerkar, K.: Medicine recommendation system. Int. Res. J. Eng. Technol. **7**(3), 1658–1662 (2020)
12. Granda Morales, L.F., Valdiviezo-Diaz, P., Reátegui, R., Barba-Guaman, L.: Drug recommendation system for diabetes using a collaborative filtering and clustering approach: development and performance evaluation. J. Med. Internet Res. **24**(7), e37233 (2022)
13. Khatwani, C., Roy, S.: Security analysis of ECC based authentication protocols. In: 2015 International Conference on Computational Intelligence and Communication Networks (CICN), pp. 1167–1172. IEEE (2015)
14. Kushwaha, N., Goyal, R., Goel, P., Singla, S., Vyas, O.P.: LOD cloud mining for prognosis model (case study: native app for drug recommender system). Adv. IoT **4**, 20–28 (2014)
15. Ochoa, J.G.D., Csiszár, O., Schimper, T.: Medical recommender systems based on continuous-valued logic and multi-criteria decision operators, using interpretable neural networks. BMC Med. Inform. Decis. Mak. **21**, 1–15 (2021)
16. Peska, L.: Using the context of user feedback in recommender systems. arXiv preprint arXiv:1612.04978 (2016)
17. Roy, S.: Denial of service attack on protocols for smart grid communications. In: Research Anthology on Combating Denial-of-Service Attacks, pp. 560–578. IGI Global (2021)
18. Roy, S., Das, A.K., Li, Y.: Cryptanalysis and security enhancement of an advanced authentication scheme using smart cards, and a key agreement scheme for two-party communication. In: 30th IEEE International Performance Computing and Communications Conference, pp. 1–7. IEEE (2011)
19. Roy, S., Khatwani, C.: Cryptanalysis and improvement of ECC based authentication and key exchanging protocols. Cryptography **1**(1), 9 (2017)
20. Roy, S., Morais, F.J.A., Salimitari, M., Chatterjee, M.: Cache attacks on blockchain based information centric networks: an experimental evaluation. In: Proceedings of the 20th International Conference on Distributed Computing and Networking, pp. 134–142 (2019)
21. Roy, S., Rudra, A., Verma, A.: An energy complexity model for algorithms. In: Proceedings of the 4th conference on Innovations in Theoretical Computer Science, pp. 283–304 (2013)
22. Roy, S., Rudra, A., Verma, A.: Energy aware algorithmic engineering. In: 2014 IEEE 22nd International Symposium on Modelling, Analysis & Simulation of Computer and Telecommunication Systems, pp. 321–330. IEEE (2014)

Recall-Driven Precision Refinement: Unveiling Accurate Fall Detection Using LSTM

Rishabh Mondal and Prasun Ghosal(✉)

Indian Institute of Engineering Science and Technology, Shibpur, Howrah 711103, WB, India
p_ghosal.it@faculty.iiests.ac.in

Abstract. This paper presents an innovative approach to address the pressing concern of fall incidents among the elderly by developing an accurate fall detection system. Our proposed system combines state-of-the-art technologies, including accelerometer and gyroscope sensors, with deep learning models, specifically Long Short-Term Memory (LSTM) networks. Real-time execution capabilities are achieved through the integration of Raspberry Pi hardware. We introduce pruning techniques that strategically fine-tune the LSTM model's architecture and parameters to optimize the system's performance. We prioritize recall over precision, aiming to accurately identify falls and minimize false negatives for timely intervention. Extensive experimentation and meticulous evaluation demonstrate remarkable performance metrics, emphasizing a high recall rate while maintaining a specificity of 96%. Our research culminates in a state-of-the-art fall detection system that promptly sends notifications, ensuring vulnerable individuals receive timely assistance and improve their overall well-being. Applying LSTM models and incorporating pruning techniques represent a significant advancement in fall detection technology, offering an effective and reliable fall prevention and intervention solution.

Keywords: Fall detection · Elderly care · Accelerometer sensors · Healthier Aging · Raspberry Pi

1 Introduction

Accidental falls pose a grave global challenge, ranking as the second leading cause of unintentional injury fatalities worldwide and claiming the lives of approximately 684,000 individuals annually. This pervasive tragedy falls disproportionately on low- and middle-income countries, where over 80% of these fatal incidents occur. The elderly population, aged 60 and above, bears the brunt of these misfortunes, suffering physical harm and substantial financial implications. The costs associated with falls among the elderly are projected to rise from an estimated $20 billion in 2000 to a staggering $54.9 billion by 2020, as reported by the Centers for Disease Control and Prevention (CDC).

D. Puthal et al. (Eds.): IFIPIoT 2023, IFIP AICT 684, pp. 74–83, 2024.
https://doi.org/10.1007/978-3-031-45882-8_6

The consequences of falls extend far beyond immediate injuries, as many elderly fall victims cannot regain their footing independently, requiring assistance that may be delayed. Shockingly, individuals can wait an average of 10 min or longer, with 3% enduring an hour or more of helplessness before receiving aid. Prolonged immobility during these critical periods often leads to further health complications, hospitalizations, institutionalization, and increased morbidity and mortality rates. Given these alarming statistics, it is crucial to implement comprehensive prevention strategies that combine education, training, secure environments, and innovative research initiatives supported by effective policy interventions to mitigate fall risks.

Existing literature offers numerous strategies to reduce fatal falls and improve the response times of medical and nursing staff. However, many of these solutions face high costs, complex implementations, or privacy limitations. To address these obstacles, we present a cost-effective embedded fall detection device that leverages accelerometers and gyroscopes, providing an unparalleled user-friendly experience. Our research endeavours encompass pioneering ideas, including developing a wearable node integrating fall detection, victim localization, and staff notification functions into a single device. Additionally, we introduce a robust and reliable Long Short-Term Memory (LSTM) model meticulously compared to conventional machine learning (ML) algorithms to enhance the accuracy and efficiency of fall detection. Complementing these advancements, we have designed an intuitive Android application to assist caregivers in providing care and support.

By merging cutting-edge technologies, cost-effective design, and a holistic perspective on fall detection and prevention, our research aims to alleviate the burden of falls, empower caregivers, and enhance the overall well-being of vulnerable individuals. Our comprehensive approach addresses the pressing need for effective fall prevention strategies, offering promising avenues to mitigate risks and improve the outcomes for fall victims.

2 Literature Survey

This chapter focuses on the design of a fall detection system for monitoring geriatric healthcare and detecting falls. Figure 1 demonstrates various Fall Detection systems.

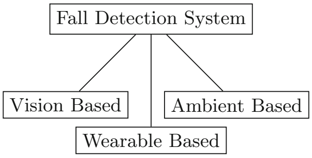


Fig. 1. Various types of a Fall Detection System

- **Vision-Based System**

Anishchenko [2] deep learning and transfer learning methodologies on real-world surveillance camera data to identify instances of falls to address the limitations associated with artificially generated datasets obtained from controlled scenarios. Bhandari et al. [9] utilize a three-step approach to detect falls in video frames, comprising identifying interest points through the Shi-Tomasi algorithm, determining the inter-point distances by calculating optical flow with the Lucas-Kanade algorithm and estimating motion speed and direction to determine the occurrence of falls. Ogden Kwolek [7] analyzed Kinect camera feeds and utilized point cloud images to detect falls.

Vision-based systems in healthcare offer precise information through images or video feeds, aiding remote caregivers and enabling early detection of health issues. However, they can be costly to implement and maintain, time-consuming to process, and raise privacy concerns.

- **Ambient-Based System**

Taramasco et al. [11] describes a fall classification system that utilizes low-resolution thermal sensors placed at two horizontal planes near the floor. The results revealed that the Bi-LSTM model achieved a high accuracy of 93%, outperforming the other RNN models.

This ambient system offers several advantages, including its comfortable nature as it does not require users to wear any devices or sensors. It enables continuous monitoring, even without the user wearing any sensors. In case of disadvantages, False alarms may also occur if certain activities are misinterpreted as falls, such as when the user is sitting or lying down.

- **Wearable-Based System**

Kaewkannate and Kim [6] comprehensively analyze four wearable devices designed in a wristband style. Their evaluation thoroughly compares each device's various features and costs. On the other hand, the power consumption of wearable devices is highly dependent on several factors. He et al. [8] combined tri-axial accelerometers with gyroscopes and magnetometers to capture a comprehensive range of motion data. Their wearable device demonstrated enhanced performance in detecting falls and differentiating them from everyday activities.

Wearable fall detection devices offer increased safety and improved response time, particularly for individuals at risk of falls. They have a user-friendly design and are often more cost-effective than alternative caregiving options. However, these devices may be prone to false alarms and have limited effectiveness in detecting certain types of falls, posing user challenges.

3 Preliminaries

3.1 Problem Statement

The growing concern about falls among the elderly necessitates the development of accurate and practical fall detection systems. Vision-based and ambient-based approaches have limitations in terms of accuracy and practicality. Wearable fall detection systems offer continuous and unobtrusive monitoring, overcoming the boundaries of existing methods. However, achieving high recall while maintaining acceptable precision is a challenge. This paper aims to develop a wearable fall detection system that prioritizes high memory using sensors and LSTM models. By leveraging wearable sensor technology and LSTM models, this system aims to enhance the safety and well-being of vulnerable individuals.

3.2 Relevance of LSTM in Fall Detection

LSTM [5] is a valuable approach in fall detection, addressing precision and recall challenges. Recall is crucial in fall detection to minimize false negatives and ensure timely assistance. LSTM detects sudden sit and fall events by capturing their temporal dynamics and leveraging its memory component. Compared to methods like MLP, LSTM's ability to capture long-term dependencies enhances its effectiveness in recognizing fall patterns. Utilizing LSTM in fall detection systems can significantly improve the safety and well-being of individuals requiring monitoring (Fig. 2).

3.3 Sensor

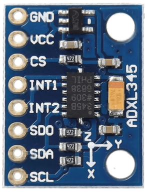


Fig. 2. ADXL345 Sensor

The ADXL345 sensor is reliable and versatile for applications requiring precise motion sensing and acceleration measurement. It offers exceptional performance with low power consumption, high resolution, and programmable range options. With its integrated 3-axis gyroscope functionality, the ADXL345 provides comprehensive motion-sensing capabilities. Its ability to accurately measure changes in acceleration makes it well-suited for fall detection applications. The sensor's low power consumption and compact size make it ideal for integration into wearable devices. The programmable features of the ADXL345 enable customization for optimizing fall detection accuracy and minimizing false alarms.

4 Proposed Methodology

4.1 Overview of Hardware System

Figure 3 provides an overview of the total system, encompassing power management, data acquisition, and communication in a mobile device. Key components include the Power Manager Unit for efficient power distribution, an accelerometer and gyroscope for accurate motion sensing, Raspberry Pi 3 B+ as the central processing unit, GPS and SIM908 modules for precise positioning, a GSM module for network communication, and a user device for interaction with the system.

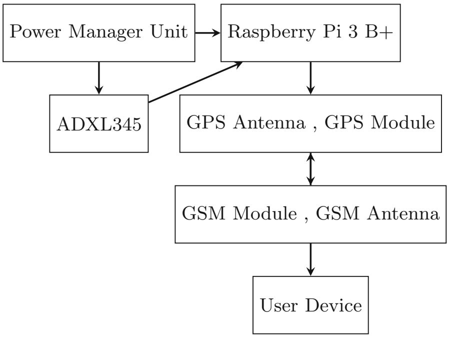


Fig. 3. Overview of the Hardware system

4.2 Data-Preprossessing

Data preprocessing enhances fall detection system performance by addressing noise, drift, and artefacts in accelerometer and gyroscope sensor data. Filtering techniques like low-pass and median filters reduce noise and outliers. Normalization scales data to a standardized range, ensuring consistent comparisons across sensors or individuals. Feature extraction identifies relevant patterns, such as statistical measures or frequency-domain features, facilitating accurate fall detection. The Butterworth filter provides a smoothing effect, highlighting significant variations in acceleration or angular velocity associated with falls: filter order and cutoff frequency selection balance precision, computational complexity, and phase distortion. Min-Max normalization eliminates biases and scaling effects, improving accuracy and robustness. Z-score normalization is an alternative technique. The choice of preprocessing methods depends on system requirements and sensor data characteristics. Figure 4 visually represents accelerometer data for a forward fall, showcasing both the raw and filtered data.

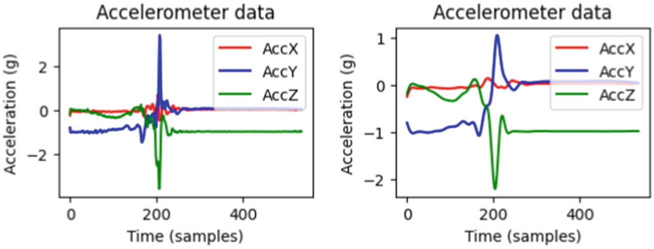


Fig. 4. Graphical representation of raw and filtered data

4.3 Proposed Model

In our research, we utilized a Long Short-Term Memory (LSTM) model, a type of recurrent neural network, for fall detection. There are two LSTM layers with 64 and 32 memory units each. This design effectively captured temporal dependencies and patterns in the accelerometer and gyroscope data, enabling accurate classification of falls. The input data for the LSTM model included accelerometer and gyroscope measurements from three axes, providing a comprehensive representation of motion data. The model processed sequences of 50-time steps, each with six features (3-axis accelerometer and 3-axis gyroscope measurements). To prevent overfitting, Dropout layers were incorporated after the LSTM layers. The LSTM model employed an output layer with two units representing fall and non-fall classes. A softmax activation function generated probabilities for each category, allowing the model to estimate the likelihood of input sequences belonging to each class. The model was trained using the categorical cross-entropy loss function to minimize the discrepancy between predicted and actual class labels. The Adam optimizer, known for adapting learning rates for individual model parameters, updated the model's weights based on computed gradients. Default parameters were employed, and a batch size 32 was used to facilitate efficient parameter updates and speed up model convergence.

4.4 Applied Weight Pruning Techniques

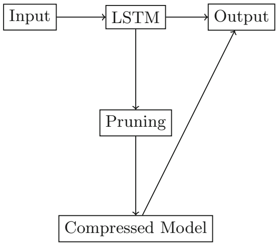


Fig. 5. Pipeline of Weight Pruning in LSTM

To optimize the LSTM model, weight pruning techniques were applied. Weight pruning involves selectively removing less significant connections or weights from the network while preserving accuracy. Figure 5 represents the pipeline of weight pruning in LSTM. The goal was to achieve a 10 to 30% pruning sparsity rate, meaning the percentage of pruned weights. Weight pruning offers benefits beyond model compression. It improves computational efficiency by reducing computations during inference. The reduced model size enables easier deployment on resource-constrained devices. Weight pruning contributes to developing efficient and lightweight fall detection systems suitable for real-world applications.

Table 1. Description of six types of ADL and four types of fall

ADL Activities		
Description	Notations	Data points
Walking	NF1	980
Sitting	NF2	1010
Lying	NF3	970
Running	NF4	1200
Sudden Sit	NF4	1100
Sudden Standing	NF5	1220

FALL Activities		
Description	Notations	Data points
Fall Forward	F1	1200
Fall Backward	F2	990
Fall Left	F3	1000
Fall Right	F4	1100

5 Result

5.1 Dataset

Table 1 represents the collected real-time data to differentiate between falls and activities of daily living (ADLs), a group of six individuals (three women and three men, aged 30 to 60) participated. Their heights ranged from 160 cm to 185 cm, and their weights varied from 50 kg to 85 kg. To achieve this goal, the participants performed six different types of ADLs and four types of falls under controlled conditions using a mattress with a thickness of 20 cm. A total of 10,770 data points were collected during the study, with 6,480 data points corresponding to ADLs and 4,290 data points corresponding to falls. The data points were collected from the participants while performing the designated activities, with variations in activity frequencies among participants. Participants A, B, C, D, and E (all aged 30) completed ten exercises each. In contrast, participants E, F (aged 55), G, H (aged 58), and I (aged 60) performed a different number of activities based on individual capabilities or study requirements.

5.2 Experimental Setup

The research utilized Anaconda with Keras and TensorFlow on Windows 10 for training LSTM models. Testing was conducted on a Raspberry Pi 3 B+ in a Linux environment. Jupyter Notebook was used for code execution and result analysis. This approach allowed for evaluating model performance on different platforms and assessing real-world feasibility.

5.3 Confusion Matrix

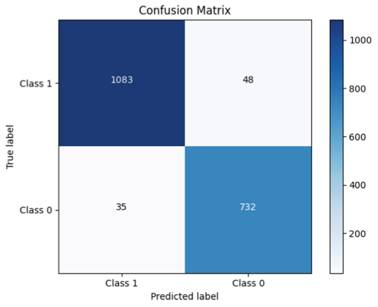


Fig. 6. Confusion Matrix

Figure 6 represents the confusion matrix for the fall detection system can be summarized as follows:

The system achieved the following in the case of non-fall instances (Class 0).1083 true negatives (TN), correctly classifying them as non-fall instances.48 false positives (FP), incorrectly classifying them as fall instances. For fall instances (Class 1), the system achieved the following. Seven hundred thirty-two true positives (TP), correctly identifying them as fall instances. Thirty-five false negatives (FN), incorrectly classifying them as non-fall instances.

This information provides valuable insights into the system's classification performance for fall and non-fall instances.

5.4 Classification Report

Class 0 (non-fall) instances were classified with 97% precision and 96% recall, resulting in an F1-score of 96%. For class 1 (fall) instances, the precision was 94%, the recall was 95%, and the F1-score was 95%. These metrics demonstrate the system's high accuracy in identifying non-fall and fall instances. Figure 7 and 8 represents train test accuracy and train test loss.

5.5 Receiver Operating Characteristic (ROC) Curve

Figure 9 displays the Receiver Operating Characteristic (ROC) [3] curve, visually representing the fall detection system's performance. The ROC curve showcases the trade-off between sensitivity (true positive rate) and specificity (1 - false positive rate) at various classification thresholds. The Area quantifies the performance of the fall detection system Under the ROC Curve (AUC). The AUC value, calculated as 0.96 in this case, accurately measures the system's ability to differentiate between fall and non-fall instances. A higher AUC value signifies a more substantial discriminatory power of the system.

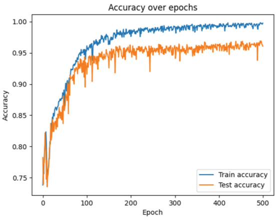


Fig. 7. Train and Test accuracy

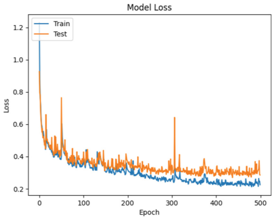


Fig. 8. Train and Test Loss

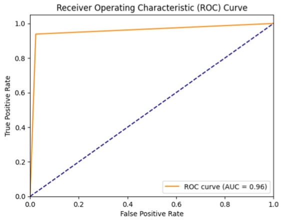


Fig. 9. ROC curve

6 Comparison of Different Models and Proposed LSTM

The comparison of different models involved assessing their performance based on various metrics such as accuracy, precision, and recall. Table 2 presents valuable insights into the models' performance in accurately classifying fall and non-fall instances while effectively reducing false positives and negatives.

(A - Accelerometer, G - Gyroscope, N/A - Not Applicable)

Table 2. Fall Detection Systems Comparison

References	Sensors	Algorithm	Sensitivity	Specificity
Shi et al. [10]	A	SVM	90.0	95.7
Aguiar et al. [1]	A	Dec. Tree	94.0	90.2
Helmy and Helmy [4]	A	Thresholds	95.0	90.0
Tran et al. [12]	A	Perceptron	60.4	94.8
Proposed Model	A, G	LSTM	95	96

7 Conclusion and Future Work

This research addressed the critical issue of fall-related incidents by developing and evaluating a fall detection system using LSTM. The system achieved high accuracy, precision, and recall, effectively minimizing false negatives. The LSTM-based system demonstrated competitive accuracy, sensitivity, and specificity performance compared to previous models. Future research directions include model optimization, sensor integration, real-time implementation, dataset expansion, and validation in real-world scenarios. Overall, this thesis improves the safety and quality of life for individuals at risk of falls. Future research should focus on utilizing more lightweight sensors and incorporating additional features to improve the accuracy of the fall detection system.

References

1. Aguiar, B., Rocha, T., Silva, J., Sousa, I.: Accelerometer-based fall detection for smartphones. In: 2014 IEEE International Symposium on Medical Measurements and Applications (MeMeA), pp. 1–6. IEEE (2014)
2. Anishchenko, L., Zhuravlev, A., Chizh, M.: Fall detection using multiple bioradars and convolutional neural networks. Sensors **19**(24), 5569 (2019)
3. Fawcett, T.: An introduction to ROC analysis. Pattern Recogn. Lett. **27**(8), 861–874 (2006)
4. Helmy, A., Helmy, A.: Seizario: novel mobile algorithms for seizure and fall detection. In: 2015 IEEE Globecom Workshops (GC Wkshps), pp. 1–6. IEEE (2015)
5. Hochreiter, S., Schmidhuber, J.: Long short-term memory. Neural Comput. **9**(8), 1735–1780 (1997)
6. Kaewkannate, K., Kim, S.: A comparison of wearable fitness devices. BMC Pub. Health **16**, 1–16 (2016)
7. Kwolek, B., Kepski, M.: Fall detection using kinect sensor and fall energy image. In: Pan, J.-S., Polycarpou, M.M., Woźniak, M., de Carvalho, A.C.P.L.F., Quintián, H., Corchado, E. (eds.) HAIS 2013. LNCS (LNAI), vol. 8073, pp. 294–303. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-40846-5_30
8. Ranakoti, S., et al.: Human fall detection system over IMU sensors using triaxial accelerometer. In: Verma, N.K., Ghosh, A.K. (eds.) Computational Intelligence: Theories, Applications and Future Directions - Volume I. AISC, vol. 798, pp. 495–507. Springer, Singapore (2019). https://doi.org/10.1007/978-981-13-1132-1_39
9. Sase, P.S., Bhandari, S.H.: Human fall detection using depth videos. In: 2018 5th International Conference on Signal Processing and Integrated Networks (SPIN), pp. 546–549. IEEE (2018)
10. Shi, Y., Shi, Y., Wang, X.: Fall detection on mobile phones using features from a five-phase model. In: 2012 9th International Conference on Ubiquitous Intelligence and Computing and 9th International Conference on Autonomic and Trusted Computing, pp. 951–956. IEEE (2012)
11. Taramasco, C., et al.: A novel monitoring system for fall detection in older people. IEEE Access **6**, 43563–43574 (2018)
12. Tran, H.A., Ngo, Q.T., Tong, V.: A new fall detection system on android smartphone: application to a SDN-based IoT system. In: 2017 9th International Conference on Knowledge and Systems Engineering (KSE), pp. 1–6. IEEE (2017)

Blockchain for IoT-Driven Systems (BIoT)

Application of Blockchain Based e-Procurement Solution for Mitigating Corruption in Smart Cities Using Digital Identities

Arish Siddiqui(✉), Kazi Tansen, and Hassan Abdalla

University of East London, Docklands, London, UK
{a.siddiqui,k.tansen,h.abdalla}@uel.ac.uk

Abstract. Procurement is an important governance tool that is used by the government and development agencies globally to manage and fulfil their complex development plans. However, corruption is a persistent and pervasive issue that hinders ethical progress and it can have a detrimental effect on the outcome of the proposed project that involves more than a few stakeholders. The implementation of Blockchain based e-procurement has been suggested as the potential solution due to its underlying characteristics of immutability and disintermediation. Blockchain technology utilizes distributed consensus, offering evident advantages to procurement by using the digital identities of the stakeholders in the bidding process and maintaining the privacy and security of the contract. This paper systematically maps and implements the existing literature to comprehend the utilization of Blockchain technology in the procurement domain and its potential to mitigate corruption in tender-based environments in smart cities by using digital identities.

Keywords: Blockchain · Digital Identities · Procurement · Smart Cities · Smart Contracts

1 Introduction

Corruption in the procurement process has made countless international headlines in recent years. Due to its complexity and length, the traditional procurement route exhibits a lack of transparency that exposes the potential for corruption. The processes and actions involved in procuring supplies, services, or items from any external supplier or source are referred to as procurement [1]. The procurement process is considered to be a challenging organizational process that involves several functional areas or divisions. Moreover, for effective administration of the entire process, significant amounts of organizational resources are often required. Tenders are habitually prone to the possibility of corruption because of the convoluted nature of the traditional procurement procedure. Contiguous alliances between public sector representatives and outside sources or commercial groups exacerbate the susceptibility to corruption in public procurement,

Published by Springer Nature Switzerland AG 2024
D. Puthal et al. (Eds.): IFIPIoT 2023, IFIP AICT 684, pp. 87–100, 2024.
https://doi.org/10.1007/978-3-031-45882-8_7

suggests a report released by the Organization for Economic Co-operation and Development [2]. The study established that corruption in the procurement process is the second-most prevalent kind of economic crime to be reported globally. According to an analysis by Transparency International, corruption in public procurement has the regrettable ability to aggrandize the cost of any public project by 50%, which in turn plunges the quality of the product [3]. Many organizations worldwide have implemented a variety of techniques over the years to establish transparency and mitigate corruption in both public and private areas of procurement. However, because of the centralized and intricate nature of the procurement process, corruption in the industry is still very much an obstacle. Blockchain is drawing a lot of attention from researchers due to the transparency, immutability, convenience and reliability of this technology. The decentralized construction of this technology endows a distributed consensus where data is immutable and transactions are verifiable. As a result, the benefits of transparency, efficiency, security, flexibility, cost-effectiveness, and many more may be flawlessly attained with the precise application of Blockchain. This paper confers Blockchain technology with an emphasis on its accessibility and expediency in consort with proposing a Blockchain-based approach incorporating Digital Identity to mitigate corruption in the procurement procedure.

2 Research Methodology

The authors decided to combine the qualitative and non-experimental research methods in order to perform the study. It is typical practice in the research sector to collect and analyze data using qualitative research to understand pertinent ideas [4]. In qualitative research, relevant entities are examined in their natural environments when data may not be available in numerical form. This method is empirical and is physiognomically focused on seeking the answer through “why” and “how” based examination [5]. Qualitative research allows for the adaptability of data gathering and investigation as new ideas emerge. This method allows for the exhuming of unique issues since data collection takes place in realistic settings. Besides, a secondary research technique was adopted to carry out the qualitative research study. Since this procedure is intended to synthesize previous findings for methodical examination, it provides those conducting the studies with the opportunity to appreciate the work already done in the relevant sphere and develop embryonic investigational maneuvers by using the information. The use of secondary research facilitates insight to be attained by carefully examining earlier or existing research, which is important for conducting a unique study. This research approach can be advantageous in achieving the project’s goals since it is indispensable to apprehend the scope of Blockchain technology to address the concerns with corruption, transparency and security in the procurement itinerary. Contrarily, non-experimental research allows researchers to appraise factors that occur spontaneously without external interference. This approach can be utilized when the study area is extensive and exploratory, and when there is inadequate information readily available regarding the pertinent research field [6]. In this approach, non-experimental research has the ability to quantify and designate how closely related the variables are to one another. It is imperative to mention that the two main categories of non-experimental research methods are correlational research and observational research. The statistical link that exists between variables but cannot be altered is what drives correlational study. During the implementation of the observational research method, researchers perceive how the contributors behave without obtruding with the variable. In the perception of the project's goals, observational research methods can be utilized since the potential of Blockchain to address the issues is a reliable variable while Corruption or issues with transparency that arise during the procurement process are independent variables and none of the variables are subject to researcher manipulation.

3 Procurement Process

Procurement refers to an organizational procedure that involves the acquisition of products, materials or services from an outside source [7]. The services or goods that are typically acquired include but are not limited to, office supplies, fixtures, technical apparatus, raw materials, training, testing, recruiting etc. Any public organization is required to prioritize procurement because any services or products obtained through it are accounted for with money from taxpayers [8]. A trustworthy and open procurement process is indispensable to protecting the public interest and ensuring that services are provided to a high quality. The research from the Organization for Economic Co-operation and Development states that the public procurement process is the most predisposed to corrupt practices [2]. The probability of corruption is further intensified by the adjacent coalition between officials from government bodies and commercial entities. The study also highlighted that governmental procurements accounted for almost 4.2 trillion euros in expenditure in OECD nations. Evidence from a number of sources specifies that above 50% of testified incidents of foreign bribery were associated with public organizational procurements from a variety of industries including construction, transportation, information and communication technology, and so on according to foreign bribery report [9]. The likelihood of subsidiary overheads like declined foreign investment and inadequate market access upsurges when there is corruption in public procurement. According to a Transparency International report, the process of procurement is fragmented into the following four key phases that introduce diverse opportunities for corruption, including bribery, deceitful tender obedience, embezzlement, bid rigging, administrative influence on bid assessment, and misuse of power [10] (Fig. 1).

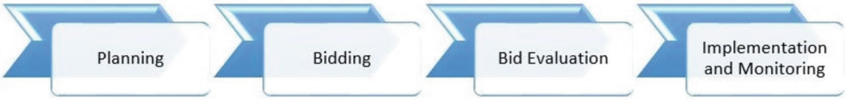


Fig. 1. Public procurement phases

A general framework may be built to comprehend the functionality even if the public procurement procedure relies on the unique government [11]. According to the requirements, a government agency normally circulates the tender description and starts the procurement procedure. The following phase is for potential participants to evaluate the specifications and submit a tender. After evaluating the submitted bids in line with the requirements set forth, the government organization decides upon the preeminent proposal. However, inadequate transparency and bureaucratic intricacy are fostering a culture of corruption in public procurement, which diminishes citizens' expectations of their government, deters foreign investment, and eventually impairs the economy [11]. As an illustration, one of the prevalent construction establishments in Latin America, 'Odebrecht', was convicted of disbursing bribes totaling almost $800 million in exchange for being awarded different public sector contracts and projects [12]. The Brazil-based engineering establishment filed for liquidation as a result of the public corruption probe. However, the preponderance of Odebrecht's debt, which had been retained by the state bank, eventually resulted in a $25.3 billion liability for Brazilian taxpayers. By creating an impartial, safe, decentralized, and trustworthy procurement architecture that is able to accomplish the entire process transparently, a corruption-free procurement system is feasible [13]. Blockchain technology has been proposed in numerous research to establish an impartial, secure, trustworthy, and transparent public procurement system where all the information, such as competitive data and tender quotation can be handled without being susceptible to exploitation or data counterplots. By facilitating a decentralized defense mechanism, Blockchain technology conserves data integrity and quality [14].

4 Blockchain

Blockchain is a type of distributed ledger that stores transaction data in units called 'Blocks'. The block that contains a link to the preceding block stores a collection of transactions. A chain of blocks in chronological sequence is created as a result [14]. The principal component of Blockchain is a distributed ledger, via which data may be added to and reformed utilizing the network's consensus process between nodes. A replica of all the records in a sequence of interconnected systems is stored on each liaising node in a Blockchain where transactions are traceable, transparent, and tamper-proof since it incorporates the utilization of a P2P network, distributed consensus, pseudonymity and cryptographic mechanisms [15]. The following figure exhibits a simplified Blockchain structure (Fig. 2).

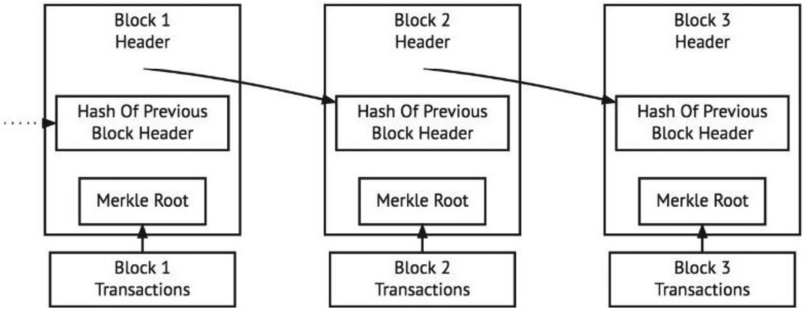


Fig. 2. Simplified Structure of Blockchain [16]

A cryptographic hash function is utilized in a Blockchain to connect consecutive blocks in such a manner that any update to the transaction data in Block 1 would modify the hash value of Block 2, which would subsequently change the hash of Block 3. In the case that the block is even slightly altered, this approach produces a readily apparent disparity [17]. Due to the enormous popularity of cryptocurrencies, Blockchain has generated a lot of interest in recent years. The idea that Blockchain is solely used for cryptocurrency is arguably the largest misperception about it [18]. As a Distributed Ledger Technology, Blockchain primarily emphasizes offering a set of protocols and procedures for the dissemination of records across several nodes in a cooperating system. The following are fundamental properties of Blockchain technology.

- **Decentralisation:** The process that makes it possible to distribute and constrain control from a centralised authority or place is known as decentralisation. Without the requirement for a reliable third party, decentralisation has the aptitude to enable transparent data exchange. The architecture of decentralised system assurances that information is maintained by all entities rather than being stored by a single one [19]. Blockchain enables resilience from a single point of failure problem since transactions are stored as blocks in a distributed P2P network [20]. Decentralisation surpasses the trust issue by empowering various nodes to administer the network.
- **Transparency:** A dynamic record of every transaction that has already taken place is available on the Blockchain, which is a distributed ledger. There are five commonly identified indispensable qualities for the foundation of transparency [21]. These are accessibility, instructiveness, usability, auditability and comprehensibility. By enabling encrypted access to the data, accessibility is provided in the Blockchain network. To validate the transaction in nodes at various networks, the processing power of Blockchain supports the aptitude of operation and performance in terms of usability. Blockchain offers permanent storage of comprehensive information in the form of blocks, where each effort at modification results in the formation of a new block that comprises a reference to the original data of the preceding block. This endorses instructiveness. By encompassing pertinent data about transactions and smart contracts, including indispensable information for forthcoming authentication in blocks, the Blockchain delivers comprehensibility. Through an algorithm that substantiates the settings and prerequisites prior to accruing new blocks, Blockchain technology guarantees auditability.
- **Immutability:** Immutability in the context of Blockchain technology refers to its ability to be unaltered and irrevocable. The consequence of the blocks that are cryptographically allied is the attribute of immutability. The processing and organisation of the information or data associated with transactions in the block are accomplished using cryptographic principles [22]. Blockchain technology makes use of the Secure Hashing Algorithm 256 (SHA-256). A hash value that consists of an alphanumeric string is generated for each block. Blocks are established to be persistent and associated together retrospectively by the fact that each block comprises a digital signature or hash value for both itself and the block before it [22].

Blockchain is a type of distributed ledger technology that makes it conceivable to record transaction details instantaneously in diverse locations. Distributed Ledger Technology, unlike traditional databases, is not reliant on centralized administration since it was not premeditated with central data storage [23]. The Distributed Ledger's nodes independently verify and process each item to construct the consensus and record of legitimacy. Cryptography is employed to safeguard the data retained on the Distributed Ledger. The ledger's structure has been constructed in a manner in which cryptographic hash functions integrate all of the nodes. Since the access method of Distributed Ledger is governed by cryptographic signatures and keys, the information's security and veracity are maintained. Applications-specific instructions are carried out via Smart Contracts on a typical Blockchain platform. Contrary to the consensus, this is not a contract in the traditional sense; rather, it is a set of instructions that has been put into operation. The self-execution and self-verification features of a smart contract can be equated to those of a computer program [24]. Any one or all of the peer nodes may host a smart contract because of its distributed and event-driven nature. The omission of any third party is made possible via a smart contract on the Blockchain, which makes the transactions autonomous. Trust obstacles can also be resolved considering there is no third party involved and transactions transpire only after the agreements are upheld.

5 Digital Identity

The concept of 'Identity' is theoretically complex. However, over the course of time, it has been characterized in numerous ways and situations. On a fundamental level, it can be argued that identity is any collection of traits that characterize an individual and can be used to specifically identify them. The digital equivalent of a person's physical identity, or the digital representation of the person, would be their digital identity as a result. According to National Institute of Standards and Technology guidelines, a digital identity is a grouping of distinctive features that distinguish an entity and specify the transactions in which it is permitted to engage [25]. The criteria for a standard digital identity include being distinct, created with the agreement of the user and verifiable with a high degree of certainty. The quantity of personal data organizations own about online consumers is expanding exponentially along with exponential technology. Organizations collect and absorb data without the users' acquaintance or consent, which is then used by third parties for data analysis, profiling, and other forms of exploitation [26]. One of the most crucial uses of Blockchain technology for numerous advancements is without any ambiguity managing and verifying digital identities. By keeping track of every transaction among identity holders and initiatives, the Blockchain ensures complete transparency at all times. The flexibility to generate an encrypted user identity that can be instantaneously accessible and used to validate identification as required is another benefit of Blockchain technology [27].

6 Smart City

The British Standards Institute defines a 'Smart City' as the efficacious incorporation of human, digital, and physical systems in the assembled settings to provide an ecological and comprehensive future for its residents [28]. The smart city is a concept that refers to the use of advanced technology and data analytics to improve the quality of life of citizens, enhance urban sustainability, and optimize the use of resources in urban areas [29]. Smart Cities integrate technology and data to manage assets, resources, and services efficiently while also promoting citizen participation and engagement. One technology that has been proposed as a potential enabler of smart cities is Blockchain. This technology can be used to enable secure and transparent transactions between citizens and government entities in smart cities. By using Blockchain, smart cities can provide a decentralized and secure platform for citizens to interact with government entities, including paying taxes, applying for permits, and voting in elections [30]. One of the main applications of Blockchain in smart cities is in the area of identity management. In a smart city, citizens will interact with a range of services and systems that require identity verification, such as transportation systems, public services, and payment systems. Blockchain can provide a secure and decentralized platform for managing identity, allowing citizens to maintain control over their data and protect them from identity theft [31]. By leveraging the security and transparency of Blockchain, smart cities can enhance the trust of citizens in the data collected and analyzed, enable secure and transparent transactions between citizens and government entities, and create decentralized marketplaces for resources in urban areas.

7 Existing solutions

A system was suggested utilizing the Ethereum platform to contrivance a smart contract as part of a Blockchain-based solution for public procurement [32]. The contributors are permitted to submit bids using their suggested system after the organizer has instigated the procurement. This approach does, however, have a few flaws. The system's access control method is one of its key drawbacks. The highest bidder among the contributors is chosen if the Reveal function is called prior to the deadline expires, which also concludes the procurement. This, however, undermines the whole procedure because neither the winner nor the procurement can be terminated before the deadline. Another procurement mechanism was constructed on the Blockchain [33]. In contrast to the earlier approach, this solution offers faultless operation up until the point of procuring bids. This approach also contains a significant flaw. The probability of tender manipulation is substantial since the system allows the organizer to personally evaluate the submitted bids which also carries the risk of corruption. An alternative smart contract for public procurement was developed, and it was constructed in such a way that it can accomplish numerous requirements for public procurement [34]. However, the system's bidding function has a significant limitation. If a new contestant bids the identical amount as the in-progress highest amount, the offer will be rejected even though it is irrational and unfair. As a consequence of this, the system fails to uphold the fundamental requirement of impartiality in the procurement process.

8 Proposed solution

Due to the traditional centralized structure, typical public procurement is a protracted and complex process with a substantial opportunity for corrupt practice. The delinquent of third-party reliance, which conveys a number of unsolicited transparency difficulties, exist in any traditional procurement system with centralized architecture

[35]. A Blockchain-based system with digital identification is suggested in light of the shortcomings of the existing systems outlined in this section (Fig. 3).

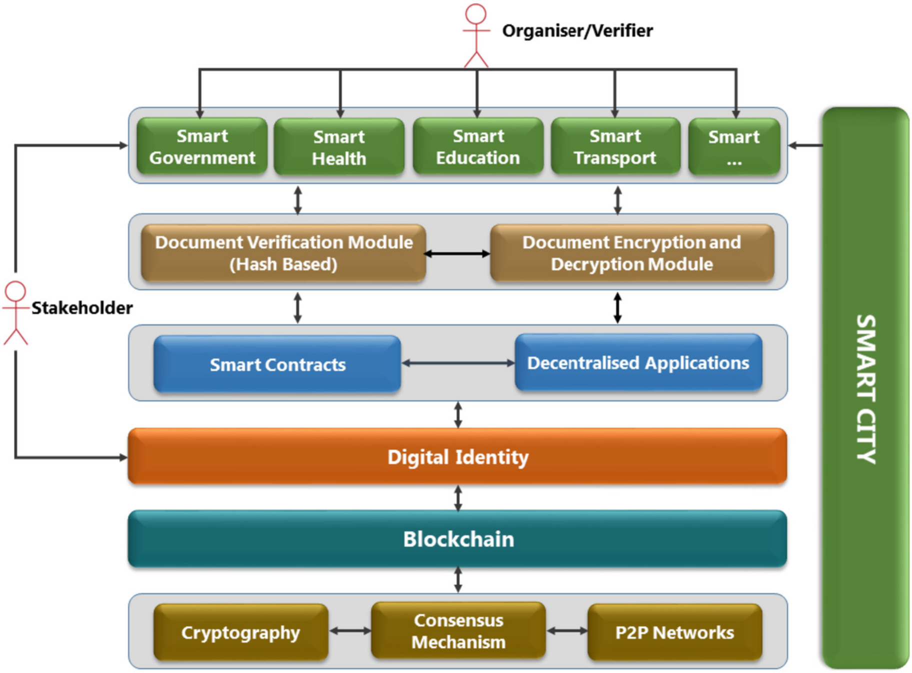


Fig. 3. Proposed Blockchain-based Solution Framework

The above figure illustrates the process of the system. The foundation layer comprises the peer-to-peer network, consensus mechanism and cryptography which provides the required decentralization and security needed to ensure transparency and trust in the process. Cryptography provides the necessary security by encrypting the data thereby preventing it from unauthorized access. The consensus mechanism safeguards that all the nodes on the network only approve the same request and the P2P network enables the direct communication between the nodes eliminating the middle tier. Above the foundation layer is the Blockchain layer which is the distributed ledger where all transactional data is stored and accessible by the stakeholders. It guarantees the traceability and transparency of the transactions and also provides the mechanism to detect any attempt to sabotage the data that has been stored on a tamper-proof and immutable distributed ledger. On top of the Blockchain layer is the Digital Identify layer in the framework where the identity of the stakeholder can be identified and validated preventing unauthorized access. Above the digital identity layer are the smart contracts and decentralized applications that are responsible for this function. Smart contracts are self-executing contracts whose terms and conditions are embedded in the code. These contracts provide leverage in automating the procurement process, including contract management, identity verification, payment processing and dispute resolution. On the other hand, decentralized applications can provide the user interface to interact with the Blockchain system. The top layer represents the elements of smart cities such as smart health, smart government, smart transport, smart education etc.

The suggested Blockchain-based solution will trigger the aforementioned procedure using smart contracts. Once the system is activated, the participant is allowed to register. Following the registration phase, the system issues a Digital ID to the participant which is required to submit the tender. The system will compare the current time to the submission deadline as the tender is being submitted. If the deadline has not passed, the participant may proceed with the submission. The subsequent phase of the process involves the system confirming whether or not the participant has already filed a tender. If no previous submission record exists, the relevant document will be encrypted followed by accepting the tender submission. However, the ability to submit a tender will no longer be available after the cut-off time. Once the deadline has passed, the documents will be decrypted. In the next phase, all of the bids will be evaluated and a winner will be declared according to the procurement policy. The Ethereum platform was chosen to create the Blockchain-based decentralized application. The Ethereum architecture makes it possible to express the network state using an account model [34]. Developers have the option to launch decentralized applications commonly known as DApps, on the Ethereum platform.

The following are some algorithms for the core functions of the solution.

Algorithm: Issue Digital Identity

```
FUNCTION generateDigitalIdentity(name, dateOfBirth, nationality, publicKey):
    digitalIdentityData = name + dateOfBirth + nationality + publicKey
    digitalIdentityHash = SHA256(digitalIdentityData)
    digitalIdentity = digitalIdentityHash
    emit DigitalIdentityGenerated(digitalIdentity)
END FUNCTION
```

This algorithm takes four input parameters - name, dateOfBirth, nationality, and publicKey - and combines them into a single string. It then hashes the combined string using SHA-256, which is a secure hashing algorithm. The resulting hash is stored on the Blockchain as a smart contract variable called digitalIdentity. Finally, the algorithm emits an event to indicate that a digital identity has been generated.

Algorithm: Encrypt Document

```
FUNCTION encryptDocument(document, encryptionKey):
    documentBytes = convertToBytes(document)
    encryptedBytes = encrypt(documentBytes, encryptionKey)
    encryptedDocument = encryptedBytes
    emit DocumentEncrypted(encryptedDocument)
END FUNCTION
```

This algorithm takes two input parameters - document and encryptionKey and converts the document into a byte array. It then encrypts the byte array using the encryptionKey, which could be a symmetric key or a public key if using asymmetric encryption. The resulting encrypted bytes are stored on the Blockchain as a smart contract variable called encryptedDocument. Finally, the algorithm emits an event to indicate that the document has been encrypted.

Algorithm: Tender Submission

```
FUNCTION submitTimedTender(tenderDetails):
    require(isTenderSubmissionAllowed(), "Tender submission is not allowed at this time")
    require(isValidTenderDetails(tenderDetails), "Invalid tender details")
    require(now < submissionDeadline, "Tender submission deadline has passed")
    tenders.push(tenderDetails)
    emit TenderSubmitted(tenderDetails)
END FUNCTION
```

This algorithm takes one input parameter tenderDetails, which is a data structure containing the details of the tender submission. The algorithm first verifies that tender submission is allowed by calling a function is TenderSubmissionAllowed(), which could check criteria such as available budget. If submission is not allowed, an error is thrown. The algorithm then verifies that the tenderDetails are valid by calling a function is ValidTenderDetails (tenderDetails), which could check criteria such as format, completeness, and eligibility. If the tender details are not valid, an error is thrown. Next, the algorithm verifies that the submission deadline has not passed by checking the current timestamp against a variable submissionDeadline which could be stored as a smart contract variable. If the submission deadline has passed, an error is thrown. If the tender submission is allowed, the tender details are valid, and the submission deadline has not passed, the algorithm adds the tenderDetails to the list of submitted tenders, which could be stored as a smart contract variable. Finally, the algorithm emits an event to indicate that a tender has been submitted.

Algorithm: Decrypt Document

```
FUNCTION decryptDocument():
    require(now >= submissionDeadline, "Tender submission deadline has not passed")
    require(!isDocumentDecrypted, "Document has already been decrypted")
    decryptedBytes = decrypt(encryptedDocument, encryptionKey)
    document = convertFromBytes(decryptedBytes)
    finalDocument = document
    isDocumentDecrypted = true
    emit DocumentDecrypted(document)
END FUNCTION
```

This algorithm assumes that the document has been previously encrypted using an encryption key and stored on the Blockchain as a smart contract variable called encryptedDocument. The algorithm first verifies that the tender submission deadline has passed by checking the current timestamp against a variable submissionDeadline which could be stored as a smart contract variable. If the submission deadline has not passed, an error is thrown. The algorithm then verifies that the document has not already been decrypted by checking a boolean variable is DocumentDecrypted. If the document has already been decrypted, an error is thrown. If the tender submission deadline has passed and the document has not already been decrypted, the algorithm decrypts the encryptedDocument using the encryptionKey. The resulting decrypted bytes are then converted back to the original document. The algorithm then sets the document as the final document, which could be stored as a smart contract variable. The algorithm also sets the isDocumentDecrypted boolean variable to true to indicate that the document has been decrypted. Finally, the algorithm emits an event to indicate that the document has been decrypted.

Algorithm: Declare Winner

```
FUNCTION determineLowestBidder():
    require(now >= submissionDeadline, "Tender submission deadline has not passed")
    require(!isWinnerDetermined, "Tender winner has already been determined")
    lowestBid = tenderList[0].bid
    FOR i = 1 TO tenderList.length - 1:
        IF tenderList[i].bid < lowestBid:
            lowestBid = tenderList[i].bid
    lowestBidder = tenderList[0]
    FOR i = 1 TO tenderList.length - 1:
        IF tenderList[i].bid == lowestBid AND tenderList[i].compliance == true:
            lowestBidder = tenderList[i]
    finalTender = lowestBidder
    isWinnerDetermined = true
    emit TenderWinnerDetermined(lowestBidder)
END FUNCTION
```

This algorithm assumes that the tenders have been previously submitted and stored on the Blockchain as an array called tenderList. Each tender in the tenderList array has a property called bid which represents the price quoted by the bidder, and a property called compliance which represents whether or not the bidder meets the compliance requirements. The algorithm first verifies that the tender submission deadline has passed by checking the current timestamp against a variable submissionDeadline. If the submission deadline has not passed, an error is thrown. The algorithm then verifies that the winner has not already been determined by checking a boolean variable is WinnerDetermined. If the winner has already been determined, an error is thrown. If the tender submission deadline has passed and the winner has not already been determined, the algorithm determines the lowest bid by iterating through the tenderList array and comparing each bid to the current lowest bid. If a lower bid is found, the corresponding bid is stored as lowestBid. The algorithm then determines the tender with the lowest bid by iterating through the tenderList array again and checking if each bid is equal to the lowestBid and if the compliance property of the bidder is true. If a tender meets these conditions, it is stored as lowestBidder. The algorithm then sets the lowestBidder as the finalTender, which could be stored as a smart contract variable. The isWinnerDetermined boolean variable is set to true to indicate that the winner has been determined. Finally, the algorithm emits an event to indicate that the winner has been determined.

9 Conclusion

The impartiality, openness, and dependability of the centralized structure raise questions that put the conventional procurement method in constant jeopardy. Numerous studies have revealed that it is challenging to set up a transparent and safe procurement strategy based on the conformist centralized architecture. This study detailed how Blockchain technology was applied to construct a trustworthy, secure, and transparent mechanism for the procurement process. The study highlighted the impediments to the conventional procurement model and elucidated its ineffectiveness. This paper evaluated the potential of Blockchain from the standpoint of mitigating procurement corruption through the functionality and usability of the technology. After evaluating the technology's potential in terms of its ability to track and regulate the transactions and records of any system at the ecosystem level, a decentralized application was generated. The decentralized platform has been reinforced by the Blockchain's physiognomies, which include transparency, immutability, security, and non-repudiation, protecting the procurement process from unlawful conduct.

References

1. What Is Procurement? https://www.investopedia.com/terms/p/procurement.asp. Accessed 15 May 2023
2. Preventing Corruption in Public Procurement. http://www.oecd.org/gov/ethics/Corruption-Public-Procurement-Brochure.pdf. Accessed 10 Jan 2023
3. Public procurement - Our priorities. https://www.transparency.org/en/our-priorities/public-procurement. Accessed 1 Feb 2023
4. What Is Qualitative Research? | Methods & Examples. https://www.scribbr.com/methodology/qualitative-research/. Accessed 15 Mar 2023
5. Punch, K.F.: Introduction to Social Research: Quantitative and Qualitative Approaches (1998)
6. Edmonds, W.A., Kennedy, T.D.: An Applied Reference Guide to Research Designs: Quantitative, Qualitative, and Mixed Methods (2012)
7. What is Procurement? https://www.hudsonprocure.co.uk/what-is-procurement-what-it-means-and-why-is-it-important-to-your-business/. Accessed 19 Jan 2023
8. Uyarra, E., Flanagan, K.: Understanding the Innovation Impacts of Public Procurement. **18**(1) (2010). https://doi.org/10.1080/09654310903343567
9. OECD Foreign Bribery Report: An Analysis of the Crime of Bribery of Foreign Public Officials. https://www.oecd-ilibrary.org/governance/oecd-foreign-bribery-report_9789264226616-en. Accessed 20 Jan 2023

10. Curbing Corruption In Public Procurement: A Practical Guide. https://www.transparency.org/en/publications/curbing-corruption-in-public-procurement-a-practical-guide. Accessed 3 Apr 2023
11. Digital Technologies for Transparency in Public Investment: New Tools to Empower Citizens and Governments. https://publications.iadb.org/en/digital-technologies-transparency-public-investment-new-tools-empower-citizens-and-governments. Accessed 10 Apr 2023
12. Reuters | Breaking International News & Views. https://www.reuters.com/. Accessed 15 Jan 2023
13. Shi, W., et al.: A Verifiable Sealed-Bid Multi-Qualitative-Attribute Based Auction Scheme in the Semi-Honest Model. **5** (2017). https://doi.org/10.1109/ACCESS.2016.2624558
14. Pereira, J. et al.: Blockchain-Based Platforms: Decentralized Infrastructures and its Boundary Conditions. **146** (2019). https://doi.org/10.1016/J.TECHFORE.2019.04.030
15. Blockchain – the gateway to trust-free cryptographic transactions. https://aisel.aisnet.org/ecis2016_rp/153
16. Bitcoin, Ethereum, Blockchain, Tokens, ICOs: Why should anyone care?, https://preethikasireddy.com/post/bitcoin-ethereum-blockchain-tokens-icos-why-should-anyone-care. Accessed 16 May 2023
17. D'Angelo, G., et al.: A Blockchain-based Flight Data Recorder for Cloud Accountability (2018). https://doi.org/10.1145/3211933.3211950
18. Biswas, S., et al.: Blockchain for E-Health-Care Systems: Easier Said Than Done **53**(7) (2020). https://doi.org/10.1109/MC.2020.2989781
19. Casey, M.J., Vigna, P.: Decentralized Blockchain Technology and the Rise of Lex Cryptographia (2015). https://doi.org/10.2139/ssrn.2580664
20. Biswas, S., et al.: GlobeChain: An Interoperable Blockchain for Global Sharing of Healthcare Data - A COVID-19 Perspective **10**(5) (2021). https://doi.org/10.1109/MCE.2021.3074688
21. Fung, A., et al.: Full Disclosure: The Perils and Promise of Transparency **27**(1), 218–221 (2007). https://doi.org/10.1002/pam.20317
22. de Leon, D.C., et al.: Blockchain: Properties and Misconceptions **11**(3) (2017). https://doi.org/10.1108/APJIE-12-2017-034
23. Lenz, R.: Managing Distributed Ledgers: Blockchain and Beyond (2019). https://doi.org/10.2139/SSRN.3360655
24. Christidis, K., Devetsikiotis, M.: Blockchains and Smart Contracts for the Internet of Things **4** (2016). https://doi.org/10.1109/ACCESS.2016.2566339
25. Grassi, P.A., et al.: Digital Identity Guidelines. National Institute of Standards and Technology (U.S.) (2017)
26. Maresova, P., et al.: Technological Solutions for Older People with Alzheimer's Disease: Review **15**(10) (2018). https://doi.org/10.2174/1567205015666180427124547
27. Rathee, T., et al.: A Systematic Literature Mapping on Secure Identity Management Using Blockchain Technology (2021). https://doi.org/10.1016/J.JKSUCI.2021.03.005
28. PAS 181 The Smart City Framework - Smart City Concept Model. https://www.bsigroup.com/en-IN/smart-cities/Smart-Cities-Standards-and-Publication/PAS-181-smart-cities-framework/. Accessed 16 May 2023
29. Caragliu, A., et al.: Smart Cities in Europe. **18**(2) (2011). https://doi.org/10.1080/10630732.2011.601117
30. Böhme, R., et al.: Bitcoin: Economics, Technology, and Governance **29**(2) (2015). https://doi.org/10.1257/JEP.29.2.213
31. Ferraro, P., et al.: Distributed Ledger Technology for Smart Cities, the Sharing Economy, and Social Compliance **6** (2018). https://doi.org/10.1109/ACCESS.2018.2876766
32. Chen, Y., et al.: Blockchain based Smart Contract for Bidding System pp. 208–211 (2018). https://doi.org/10.1109/ICASI.2018.8394569

33. Mali, D., et al.: Blockchain-based e-Tendering System (2020). https://doi.org/10.1109/ICICCS48265.2020.9120890
34. Kumar, B., Kumar, K.: Blockchain Based Smart Contract for Sealed-Bid Auction (2019). https://doi.org/10.35940/ijeat.F8083.088619
35. Yutia, S., Rahardjo, B.: Design of a Blockchain-based e-Tendering System: A Case Study in LPSE (2019). https://doi.org/10.1109/ICISS48059.2019.8969824

Blockchain Based Framework for Enhancing Cybersecurity and Privacy in Procurement

Arish Siddiqui(✉), Kazi Tansen, and Hassan Abdalla

University of East London, Docklands, London, UK
{a.siddiqui,k.tansen,h.abdalla}@uel.ac.uk

Abstract. An imperative issue that impedes economic, social, and environmental progress is the involvement of the middle tier in public institutions. Due to inadequate transparency and clandestineness in establishments, the trust in procurement process has become a predominant concern that affects many nations around the world. Governments across the globe have begun exploring cutting-edge technologies to improve procurement transparency and integrity. Blockchain is an emerging technology that comprises the potential for generating substantial advancement in the public procurement domain by establishing transparent, immutable, and autonomous processes. Even though contributions are constantly rising, adequate research and implementation are pivotal in order to fully comprehend the technology to attain these advantages. In this study, the typical procurement process was examined to evaluate the associated issues and how the digitization of the process through Blockchain technology can mitigate them by using digital identities towards maintaining the security and privacy of the entity.

Keywords: Blockchain · Framework · Cybersecurity · Procurement · Smart Contract

1 Introduction

One of the indispensable governance tools in the public sector that plays a vital role in development is public procurement. The state as well as the agencies that deal with development and funding employ the procurement process to accomplish the agendas of development [1]. Public procurements are observed to be utilized globally for escalating productivity in the public sector. However, this commendable economic mechanism is habitually distorted by corruption [2]. Due to the number of financial resources entailed, its multi-participants character and the conventional impenetrability in terms of the flow of information and the decision-making surrounding procurement, it is exclusively susceptible to corruption [3, 4].

2 Problem Definition

The effects of corruption in the public domain are enormous, and when it is not adequately controlled, it hinders the progress of a country and has a detrimental influence on citizens' quality of life through intensifying inequality, poverty, and segregation [4].

D. Puthal et al. (Eds.): IFIPIoT 2023, IFIP AICT 684, pp. 101–113, 2024.
https://doi.org/10.1007/978-3-031-45882-8_8

Typically, the misapplication of funds envisioned for the delivery of basic and important services to the population is the root cause of corrupt activities in public organizations [5]. As opposed to widespread inference, corruption in the public sector is a global indisposition. Correspondingly, deliberate attempts have always been made to choose the optimal course of action. According to the Organization for Economic Co-operation and Development (OECD), 20–25% of public procurement expenditures are drained by corruption, which reduces competitiveness, impedes the development and welfare of the general population, and ultimately undermines public confidence in government [6]. A number of strategies were also suggested by the OECD, one of which is the implementation of e-procurement, or rather digitizing the procurement process [6].

Across the globe, Governments have started implementing new technology into practice to enhance the reliability, efficacy, and financial value of their procurement procedures. However, among these technologies, Blockchain is predicted to demonstrate great potential in mitigating ineffectiveness and corrupt practices. It appears to be a perfect ally for anti-corruption due to its fundamental characteristics of disintermediation and immutability. The self-executing and autonomous Smart Contract is regarded as a persuasive instrument for efficacy and reliance since it reduces the potential for human intervention, mistakes, and preferences in taking decisions. The environment offered by the Blockchain network is known as '*Trust-less*' which indicates that transactions are not dependent on a centralized or single authority [7]. A Blockchain is a network of computer systems that replicates and distributes a digital record of transactions throughout the entire network without compromising the security and privacy of the entity. Each block on the chain comprises several transactions and each participant's ledger receives a copy of each new transaction that takes place on the Blockchain. Information, cryptocurrencies, or digital assets can all be exchanged between two system users as part of a transaction. A mechanism known as Consensus is used by network peers to vote on the legitimacy of a transaction before it is included in an immutable block [8]. It is a Distributed Ledger Technology which refers to the decentralized database that is transparent, immutable, and shared by multiple nodes. Additionally, Blockchain technology is regarded as useful because it permits a distributed consensus where every online transaction involving digital assets for any period can be verified at any time. Since every transaction is made public eliminating the possibilities of deception, Blockchain technology in procurement can offer distinct advantages that may be employed to a great outcome in the procurement function. Therefore, the typical procurement process was studied in the light of Blockchain through a methodical mapping of the existing literature to comprehend this technology in the procurement domain and a framework was proposed for enhancing security and privacy.

3 Research Methodology

In order to identify the most recent research in Blockchain, predominantly in the procurement domain, a comprehensive literature review is crucial. A systematic methodology regarding the documents of the investigative framework is also indispensable to endorse the traceability of the accomplished literature analysis. For this study, a specific method was observed for performing a comprehensive literature mapping to find techniques relating to Blockchain solutions in the multiparty sphere. A systematic literature mapping aims to measure the evidence and illustrate the area of interest through a synopsis of the literature [9]. Additionally, it is crucial to use a well-organized literature analysis to describe the current status of the research. For the analysis of literature, a concept matrix was also utilized to segment the concepts correlated to the topics into diverse units as recommended by Watson [10]. Different content criteria must be used for the amassed sources to properly classify the literature in the concept matrix. The criteria refer to the functions of Blockchain technology and procurement process management. To conduct the research, an associated link to Blockchain technology was established. In addition, key characteristics of procurement processes were ascertained followed by summarizing the comprehensions accomplished from the identified body of literature.

4 Procurement

Typically, the procedure used to get products and services from a third party as part of a contractual arrangement is referred to as procurement [1]. The fundamental objective is to obtain an unsurpassed promising rate while satisfying the buyer and seller's identity, time, quality, quantity, and locational requirements. Public procurement will therefore refer to the procedure by which the government or public sector establishments acquire merchandise and services directly to satisfy the primary requirement obligatory to assist in carrying out its core tasks of providing services or pursuing the welfare of the public [1]. The economy of any nation depends heavily on public procurement, which also serves as a primary instrument of economic expansion [2]. It often involves a series of phases such as the evaluation of requirements, contract award, procedure of contract management and payment [6]. In general, there are seven steps in the procurement process [11]. To establish a clear understanding of procurement, the procedure phases are required to be analyzed in further depth (Fig. 1).

The Spend Analysis phase is focused on cumulating historical information on products, business sector stipulation and corporate expenditure. The objective of data accumulation within an organization is to promote a mutual knowledge of previous spending. On the contrary, Demand Management concentrates on predicting client consumption as well as tracking and managing the items that are obtained. The objective of Category Management is to comprehend the requirements of stakeholders and equate them to external industry data, supplier capabilities and probable risks. In this context, a strategy is generated to balance internal prerequisites with the external aspects of the procurement market. Procurement falls under contract administration and deals with contract drafting and supplier negotiations. Other corporate divisions frequently aid with buying, allowing it to supervise the entire process while also frequently serving as a liaison between them. Cost management is another crucial aspect of procurement, through which continuous cost improvement can be achieved. In this phase, the contemplation is given to the physical goods or services to be purchased across the whole life-cycle of the product in order to accomplish persistent cost-target optimization. The streamlining of transaction operations for the acquisition of an item or service is the main emphasis of the Procure-to-Pay process step. This encompasses all arrangements, including those related to order placing, endorsement, product receipt and payment release mechanisms. The

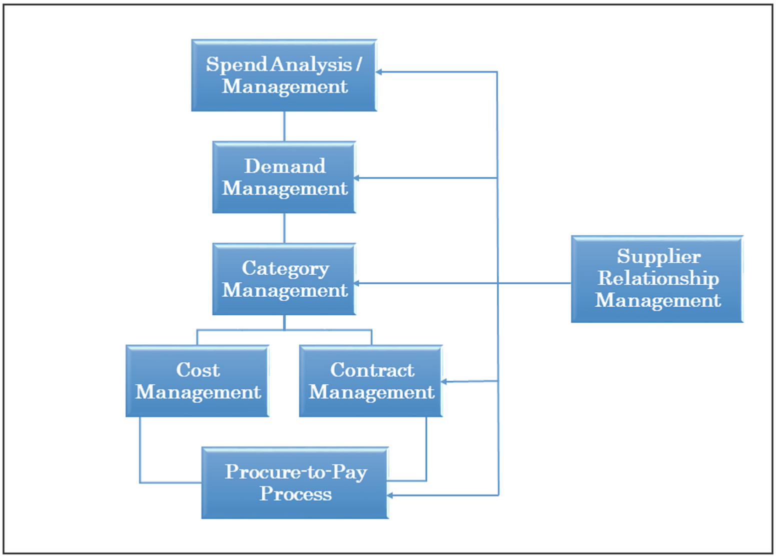


Fig. 1. Seven phases of the procurement process [10]

final phase of procurement is Supplier Relationship Management (SRM) which refers to the end-to-end process for monitoring and assessing suppliers during the procurement lifecycle. This comprises every feature of a supplier's operations including transactions, risk assessment, performance evaluation, reduce expenditures and probabilities to increase value [11]. In order to comprehend the public procurement process, the Organization for Economic Co-Operation and Development established the following three major phases for the public procurement cycle [12].

- **Pre-Tender Phase:** The procurement budget should be determined in accordance with the products, services and works that the contracting authorities anticipate requiring over a specific period of time, after which the requirement's value is determined. The requirement is then further clarified. Subsequently, the detailed specification of the procurement subject is created and the optimum procurement process is chosen.
- **Tender Phase:** According to the specified plan, the contracting authority issues the request for bids, and assesses them following the criteria stated in the request. Following the review, the contract is assigned to one or multiple bidders in line with the process.
- **Post-Tender Phase:** The monitoring of the contract's execution with all rights and responsibilities resulting from the signed contract transpires in the final phase.

As procurement incorporates all departments and functional areas of a business, the process is seen to be one of the most complex ones. Research suggests that the lack of transparency contiguous to the internal phase is one of the factors contributing to the high rates of corruption in public procurements [13]. It is common for vendors and public agents to enter unofficial, unlawful arrangements that favor some bidders when documents like the requirements assessment and the contract specification are established.

Additionally, each level of the procurement process might present the potential for persistent procurement corruption since all stakeholders have an opportunity to profit from counterfeit invoicing and bribery arrangements to inventory larceny and inferior merchandise. Public procurement corruption often involves the distorting of the process's essential competitive nature, the violation of other criteria such as the predominating public interest, manipulation or disclosure of the bids and the purpose to redirect public funds [14]. It was also emphasized that there must be indicators of intentional actions to undermine the procurement's competitive nature for obtaining unfair benefits to detect deceptions in the public procurement process. The report published by WEF also delineated some common forgery involving public procurement that can transpire during each of the three key stages of the process. For example, the corruption that takes place during the ratification of the request, agreement preparation and vendor selection [13].

Blockchain has evolved into an encouraging research technology in recent years. A report confirmed that to increase transparency in public transactions, the Justice Ministry of Ukraine conducted a Blockchain-based pilot auction [15]. The trial's major objective was to upsurge the security and transparency of the current process wherefore the data could be publicly verified. Hence, any data corruption or manipulation may be abolished. Blockchain is a distributed ledger technology which ensures that streamlining of information is independent and seamless as well as allows replication to materialize in real-time to all nodes in the system. Its foundation is to guarantee that the exchange of decentralized information and data is stored in a secure way to enable transparency, efficiency and accountability. The Blockchain may facilitate distributed and shared record possession, tamper-proofing and independent validation. In addition, numerous stakeholders can come to a covenant on items of interest in a transparent manner, reassuring transparency, efficacy, and increased feasibility of the procedure [16]. Decentralized data storage on several nodes allows independent data updating in each node, which also stimulates transparency and data security as all nodes have access to identical data. Since Blockchain Technology contains a great potential to intensify the efficacy of procurement procedures and assist in their automation, the application capacities and basics of the technology are discussed in the next section (Fig. 2).

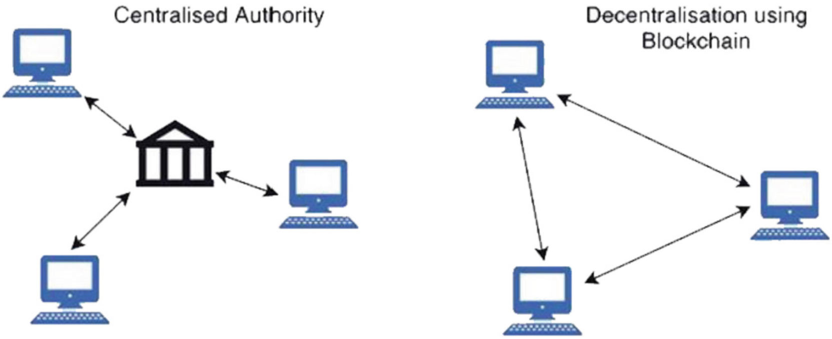


Fig. 2. Centralised and Decentralised network [33]

5 Blockchain Technology

The various application areas of Blockchain Technology are emphasized in numerous scientific literature where Blockchain was described as a distributed, decentralized, tamper-proof and collaboratively operated data storage [7]. It is vital to comprehend the underlying perceptions of Blockchain to realize, how this technology can be advantageous over conventional technologies. The introduction of the cryptocurrency known as Bitcoin by an unidentified entity '*Satoshi Nakamoto'* has gained substantial attention for Blockchain technology throughout the globe [17]. This is a technology that is rapidly evolving in the areas of innovation and application which are also experiencing diverse research. By providing decentralized defense, Blockchain technology conserves the quality and integrity of data. Characteristically, the Blockchain is a distributed database with every node holding a complete copy of the entries on the strength of the decentralized architecture [18]. In this peer-to-peer network, distributed nodes are used for data access, validation, and transmission. Peer-to-Peer networks are a precise type of distributed system that enables resource allocation between an individual node and other systems linked to the network without the prerequisite for centralized management. Blockchain is a type of distributed ledger that preserves track of transactions in units known as '*Blocks*'. The block that has a connection to the preceding block stores a collection of transactions [19]. Correspondingly, a chain of blocks in chronological sequence is generated. Blockchain technology is constructed on several fundamental concepts such as Cryptography, Consensus Game Theory, Graph Theory and Peer-to-Peer Networks [20].

- Cryptography: Within a Blockchain, data records are stored in blocks that are interconnected together by hashing algorithms and protected by asymmetric encryption.
- Consensus Game Theory: Data validation and the establishment of a single point of truth between various nodes are accomplished using Consensus Algorithms. Therefore, it is a fundamental part of decentralised systems since the elimination of central authority is conceivable.
- Graph Theory: To exemplify histories of transactions and participants of a Blockchain network in the disposition of nodes, Graphs are utilised.
- Peer-to-Peer Networks: Within a Blockchain network, information is distributed via peer-to-peer networks.

Divergent from a central database, Blockchain technology is a technological idea that uses Cryptographic techniques to store data distributed across nodes. Every collaborating peer embraces a NoSQL-based file database ledger in this distributed ledger system, which is capable of assenting a multiplicity of unstructured data [21]. In a P2P network that supports Transport Layer security, peers are associated with one another. With its distributed, decentralized, encrypted and immutable architecture, Blockchain offers a public data ledger that permits transactions concerning two parties without the requirement for a third party to function as a supervisor. In order to finalize these transactions, Digital addresses and a '*Wallet'* with private and public keys are utilized. The Blockchain typically functions as a distributed ledger where the transactions of the users are recorded in blocks. Along with the transactions, each block also comprises a *'Time-stamp*' and the preceding block's reference. A chain of blocks is created by each block's correlative reference to its precursor. Regulated by the protocol in use, the nodes connected to the network execute the Blockchain [22]. Several cryptographic techniques known as the Consensus Mechanism are utilized for block validation. An example of extensively used Consensus Mechanisms is Proof-of-Work (PoW) and Proof-of-Stake (PoS). The access depends on the configuration of the network, which may be broken down into three separate settings as Public, Permissioned and Public, Permissioned and Private [23]. It is probable for any computer to access the public Blockchain, which offers high levels of encryption and obscurity. As opposed to public Blockchain, a reduced level of obscurity is engaged and only authorized users may access the data on a private Blockchain, where the contributors are recognized by one another. Based on the core concepts, the following three functions of Blockchain technology can be emphasized [24]:

- Safeguarding the integrity of data: To secure and ensure the integrity of data, Blockchain technology provides the aptitude to verify whether database records have changed over time or not. Since the entries are associated with hash values, any alterations to the block's transactions would result in a modification in the hash, rendering the block invalid.
- Transaction processing and communication: Blockchain allows transactions amongst contributors. The reinforcement for modifications in the distributed ledger is comprised of the transaction entry and its authentication.
- Data access and registration: In the best interests of owners, Blockchain technology offers transparent and regulated access to data. Utilizing the features such as time stamps, private keys and public keys, data access is also supervised.

5.1 Data Integrity

The exchange of trustworthy data is crucial for the exact collaboration of organizations in order to complete procurement responsibilities. However, in typical procurement settings, the precise transfer of information between the participants suffers because of data storage complications and a lack of information exchange [25]. Consequently, the data offered can be incomplete, inaccurate, or altered. Due to these factors, communication costs are high and transparency is reduced [26]. However, the Blockchain can ensure data integrity, making it a viable solution to this issue. Since there is a restriction on the size of the data set in the Blockchain, it is feasible to outsource large data records and keep the hash value as a reference to the outsourced data [27]. The Merkle root is utilized to verify the data integrity by encapsulating every transaction in the block into a 256-bit annotation. A double hash algorithm is used to determine the hash value of the block's two transactions. Up until there is just one hash value left which refers to the Merkle root, this operation is repeated. This is also represented as the Merkle tree's end. The Merkle root would change because of alteration in a transaction. Therefore, it is conceivable to provide integrity verification retroactively [7].

5.2 Communication and Transactions

The linguistic difficulties, currency concerns, payment options and complicated freight paperwork de-escalate operations and raise transaction and process expenses [28].

Blockchain enables direct, cost-effective digital money transfers without the requirement of financial service providers. As a result, it is implemented to effectually manage data communication and payment operations. A smart contract may also execute payments for inbound products or the fulfilment of conditions autonomously, which would result in significant cost savings.

Smart Contracts are used to organize identities and gather data, and the data sets are available to all participants and transmitted without media disruption. Information is transmitted in a procedure that allows for the chronological passing of product and order information as well as interpretation and modification of the information among the contributors. Since the transmission of information is presently administered by a self-governing third party, transaction overheads are considerably high [29]. Conversely, without the requirement of intermediaries, Blockchain technology employs cryptographic techniques to authenticate transactions, lowering transaction costs and enhancing the security of data [30]. Smart Contracts eliminate the obligation for user interaction to complete transactions by automatically triggering payment upon fulfilment of contract requirements.

5.3 Data Access and Registry

Blockchain is a sophisticated technology with an incredibly secure platform since transactions are digitally signed and data is immutable as well as transparent. Additionally, the Blockchain is an innovative paradigm that can be utilized to track previous activities and enactment and is capable of rectifying any deficiencies via business progressions, which is challenging to ensure through conventional approaches that are feasibly time-consuming and error-prone. Research suggests that Procurement corruption has become a global crisis in recent years due to the multifaceted business process with the impediments of detecting anomalies based on traditional approaches. Besides, corruption in procurement is not a topic that can be disregarded because up to 5% of the total revenue of businesses is lost due to frauds which amount to $3.7 trillion globally and among them, procurement fraud is the most common one [31]. It is infrequent for businesses to have a qualm about their procurement team or their suppliers. Nevertheless, they cannot be allowed to take advantage of the circumstances, especially when internal control in the procurement processes is inadequate. One of the primary reasons for preventing corruption, in addition to internal control measures, is the inclusion of a third party within the procurement process cycle. Virtually all forms of corruption in procurement include the participation of a third party who may have a positive connection with either the provider or the consumer. This third party is also accused of providing some unethical benefits to either the consumer or the provider. For instance, a third party may provide the purchaser with a gift or hospitality with the anticipation that the purchaser's business will provide a financial advantage in return another can be disclosure of the bid amount. Incidents of such kind are very challenging to identify and verify the identity of the entity. However, the overriding alternative mitigation approach, technique and instrument to address such significant difficulties in the procurement process is Blockchain technology where all transactions are recorded and carried out on an immutable and secure digital ledger with no intervention from a third party and the transactions may be conducted directly between the parties with complete transparency and virtually negligible risk of deception.

5.4 Digital Identity

The theoretical complexity of the concept of *Identity* has led to numerous characterizations over time. At its core, identity can be understood as a collection of traits that define an individual and can be used for identification purposes. In the digital realm, a person's digital identity is equivalent to their physical identity and represents them in the digital space. A digital identity is a set of distinctive features that distinguish an entity and determine its authorized transactions [32]. A standard digital identity must be unique, user-agreed, and verifiable with a high level of certainty. The exponential growth of personal data collected by organizations, without users' knowledge or consent, is used for data analysis, profiling, and other exploitative practices. Blockchain technology can be used to manage and verify digital identities, enabling transparency by tracking every transaction among identity holders and initiatives. Additionally, Blockchain technology can generate an encrypted user identity that can be accessed instantly to validate identification as needed.

6 Proposed Blockchain Based Framework

Sabotage in procurement has long been a major challenge for governments and cities around the world, leading to a loss of public trust, wastage of public funds, time and overall inefficiency. However, the rise of Blockchain technology has opened new possibilities for mitigating corruption in procurement and other domains of smart cities. In this proposal, we outline a Blockchain-based framework that can be utilized in procurement as well as various domains of smart cities to ensure identity, transparency, accountability, and efficiency (Fig. 3).

The bottom layer of the framework is powered by cryptography, consensus mechanisms, and peer-to-peer (P2P) networks. These foundational elements of Blockchain technology provide the necessary security and decentralization required to ensure trust and transparency in the procurement process. By leveraging cryptography, the framework can ensure that data is encrypted and secure, preventing any unauthorized access or manipulation. Consensus mechanisms ensure that all participants in the network agree on the same version of the truth, while P2P networks enable direct communication between participants, eliminating the need for intermediaries.

On top of these foundational elements, we have the Blockchain layer. This layer acts as a distributed ledger, where all procurement-related data is stored and can be accessed by all authorized parties. This ensures that all transactions are transparent as well as traceable and that any attempt to sabotage can be detected easily. By using a Blockchain-based framework, all procurement-related data can be stored on a tamper-proof and immutable ledger, eliminating the possibility of fraud, corruption, or manipulation.

The third layer of the framework is digital identity. This layer ensures that all participants in the procurement process are properly identified and authenticated, eliminating the possibility of impersonation or unauthorized access. By leveraging digital identity, the

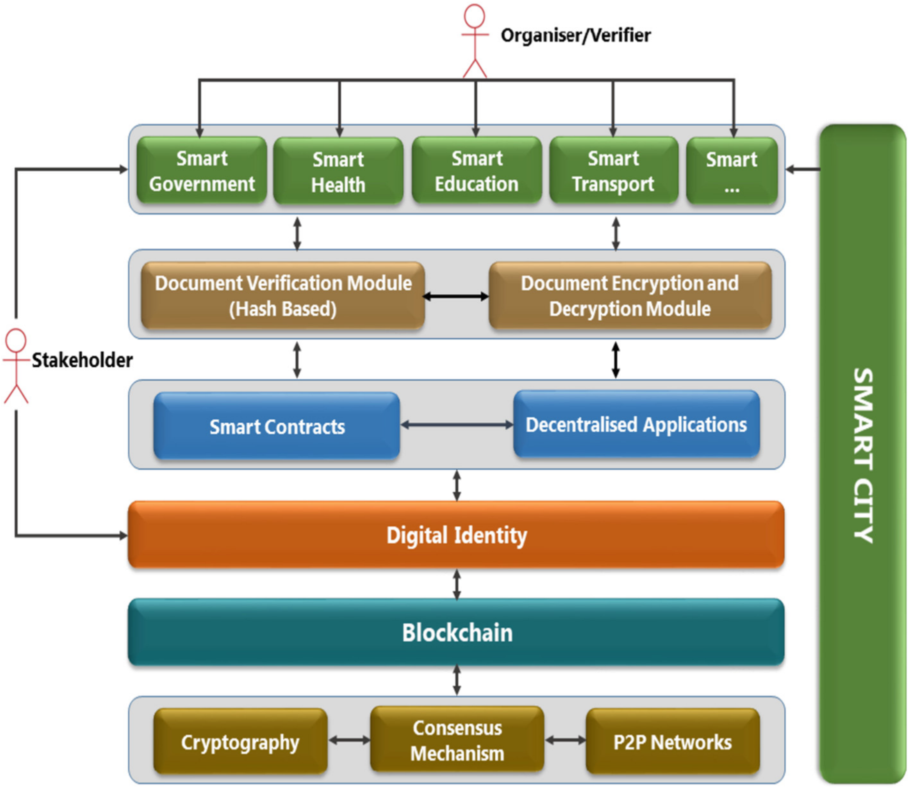


Fig. 3. Proposed Blockchain-based Framework

framework can ensure that only authorized parties have access to the procurement-related data stored on the Blockchain.

On top of the digital identity layer, smart contracts and decentralized applications carry out the function. Smart contracts are self-executing contracts with the terms of the agreement directly written into lines of code. These contracts can be used to automate various aspects of the procurement process, such as identity verification, payment processing, contract management, and dispute resolution. Decentralized applications, on the other hand, can be used to provide a user-friendly interface for accessing and interacting with the Blockchain-based procurement system.

The document encryption and decryption module on top of the smart contracts and decentralized applications layer ensures data security and privacy. When a user uploads a document, the module encrypts it using cryptographic algorithms and stores the encrypted data on the Blockchain. Access to the document is restricted to authorized parties with private keys. The decryption process allows authorized users to retrieve and view the original content securely. The document verification module validates the authenticity and integrity of stored documents. It uses smart contracts and cryptographic hashes to verify document versions against the original, ensuring data integrity and preventing unauthorized modifications, providing a *'Trust-less'* and tamper-proof ecosystem.

Finally, the top layer of the framework consists of various domains of smart cities, such as smart government, smart health, smart education, smart transport and so on. These domains can utilize the Blockchain-based procurement framework to ensure transparency, accountability, and efficiency in their respective processes.

There are several Blockchain systems available, but Bitcoin and Ethereum are the most popular ones. Since Bitcoin and Ethereum are regarded as permissionless Blockchains, anybody may join the network and publish or view transactions. If we consider the criteria for procurement, a permissionless Blockchain would be the most suitable platform in our case owing to its inherent discretion and access mechanism based on roles for accessing documents. The following advantages are made possible by the architecture we propose, which makes use of Distributed Ledger Technology's (DLT) permissionless network capabilities.

Transparent Network: The proposed structure enables the formation of exclusive communication channels among designated individuals, allowing for the unrestricted and open distribution of particular information. These channels can ensure a smooth transfer of data related to a specific product, involving key participants such as the owner, issuer, and verifier.

Uniquely Identifiable Digital Certificate: A unique hash value that uniquely identifies the owner, issuer, and verifier will be present in the digital certificate. Without altering the hash itself, this value of the hash cannot be changed. The validated document will be rejected if the hash is altered in any way since it will no longer match the original hash published on the public Blockchain.

Dispute Resolution: Any disputes relating to the information may be settled by comparing the hash of the digital data recorded on the Blockchain with the hash given by the owner, which is encoded inside the information provided by the owner.

7 Conclusion

In this study, the security concepts imperative for Blockchain procurement were discovered and explored. A Blockchain-based framework for procurement that focuses on topics is also suggested and is established on a public Blockchain network. The proposed Blockchain-based framework for mitigating corruption in procurement contains the potential to be a comprehensive solution that utilizes the latest advancements in Blockchain technology to ensure transparency, accountability, and efficiency. By leveraging the power of cryptography, consensus mechanisms, P2P networks, digital identity, smart contracts, and decentralized applications, this framework can help governments and cities around the world to mitigate corruption in procurement and other domains of smart cities. For future research, the suggested framework will be implemented in a public Blockchain network.

References

1. Ambe, I.M.: Public Procurement Trends and Developments in South Africa. **3**(4) (2016). https://doi.org/10.17261/PRESSACADEMIA.2016.351
2. Lindskog, H., et al.: Corruption in Public Procurement and Private Sector Purchasing. **7**(2) (2010). https://doi.org/10.1386/JOTS.7.2.167_1
3. Munzhedzi, P.H.: South African Public Sector Procurement and Corruption: Inseparable Twins? **10**(1) (2016). https://doi.org/10.4102/JTSCM.V10I1.197
4. Public Procurement, Corruption and Blockchain Technology in South Africa: A Preliminary Legal Inquiry. https://papers.ssrn.com/abstract=3458877
5. Kimeu, S.M.: Corruption as a Challenge to Global Ethics: the Role of Transparency International. **10**(2) (2014). https://doi.org/10.1080/17449626.2014.935982
6. Preventing Corruption in Public Procurement. https://www.oecd.org/gov/ethics/Corruption-Public-Procurement-Brochure.pdf. Accessed 16 Jan 2023
7. Knirsch, F., et al.: Implementing a Blockchain from Scratch: Why, How, and What We Learned, **1** (2019). https://doi.org/10.1186/S13635-019-0085-3
8. Biswas, S., et al.: DAAC: Digital Asset Access Control in a Unified Blockchain Based E-Health System. 01 (2020). https://doi.org/10.1109/TBDATA.2020.3037914
9. Petersen, K., et al.: Guidelines for Conducting Systematic Mapping Studies in Software Engineering: An Update. **64**(64) (2015). https://doi.org/10.1016/J.INFSOF.2015.03.007
10. Watson, R.T., Webster, J.: Analysing the Past to Prepare for the Future: Writing a Literature Review a Roadmap for Release 2.0. **29**(3) (2020). https://doi.org/10.1080/12460125.2020.1798591
11. Monczka, R.M., et al.: Purchasing and Supply Chain Management. 6th ed.. Cengage Learning (2016)
12. OECD Legal Instruments. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0411. Accessed 16 Feb 2023
13. Exploring Blockchain-based public procurement to reduce corruption. https://www.publicspendforum.net/blogs/psfeditorial/2020/06/18/exploring-blockchain-based-public-procurement-to-reduce-corruption/. Accessed 19 Jan 2023
14. Prototyping a Smart Contract Based Public Procurement to Fight Corruption. 10(7), 85. https://doi.org/10.3390/computers10070085
15. Ukrainian ministry carries out first Blockchain transactions. https://www.reuters.com/article/us-ukraine-blockchain-idUSKCN1BH2ME. Accessed 10 Mar 2023
16. Blockchain and distributed ledger technologies in the humanitarian sector. https://www.econstor.eu/handle/10419/193658. Accessed 16 May 2023
17. Auctioning Using Blockchain Advantage Analysis. https://www.ijntr.org/auctioning-using-blockchain-advantage-analysis. Accessed 01 Mar 2023
18. Sheth, H., Dattani, J.: Overview of Blockchain Technology. 05(01) (2019). https://doi.org/10.33130/AJCT.2019V05I01.013
19. Optimistic Fair-Exchange with Anonymity for Bitcoin Users. 44–51 (2014). https://doi.org/10.1109/ICEBE.2014.20
20. Rathee, T., et al.: A Systematic Literature Mapping on Secure Identity Management Using Blockchain Technology (2021). https://doi.org/10.1016/J.JKSUCI.2021.03.005
21. Biswas, S., et al.: Interoperability and Synchronization Management of Blockchain-Based Decentralized e-Health Systems. **67**(4) (2020). https://doi.org/10.1109/TEM.2020.2989779
22. Blockchain – the gateway to trust-free cryptographic transactions. https://aisel.aisnet.org/ecis2016_rp/153
23. Özdemir, A.İ., et al.: The Role of Blockchain in Reducing the Impact of Barriers to Humanitarian Supply Chain Management. **32**(2) (2021). https://doi.org/10.1108/IJLM-01-2020-0058

24. Blockchain Technology in Procurement - A Systematic Literature Mapping. 7–13. https://doi.org/10.48446/opus-11859
25. Chopra, S., Meindl, P.: Supply Chain Management: Strategy, Planning & Operation (2007)
26. Cachon, G.P., Fisher, M.L.: Supply Chain Inventory Management and the Value of Shared Information. **46**(8) (2000). https://doi.org/10.1287/MNSC.46.8.1032.12029
27. O'Leary, D.E.: Configuring Blockchain Architectures for Transaction Information in Blockchain Consortiums: The Case of Accounting and Supply Chain Systems. 24(4) (2017). https://doi.org/10.1002/ISAF.1417
28. Gunasekaran, A., Ngai, E.: Information Systems in Supply Chain Integration and Management. **159**(2) (2004). https://doi.org/10.1016/J.EJOR.2003.08.016
29. Wang, Z., et al.: Blockchain-based Framework for Improving Supply Chain Traceability and Information Sharing in Precast Construction. **111** (2020). https://doi.org/10.1016/J.AUTCON.2019.103063
30. Abidi, M.H., et al.: Blockchain-based Secure Information Sharing for Supply Chain Management: Optimization Assisted Data Sanitization Process. **36**(1) (2021). https://doi.org/10.1002/INT.22299
31. How emerging technologies are helping tackle procurement frauds. https://www.ey.com/en_in/forensic-integrity-services/how-emerging-technologies-are-helping-tackle-procurement-frauds. Accessed 16 May 2023
32. A Systematic Literature Mapping on Secure Identity Management Using Blockchain Technology. https://www.neliti.com/publications/429349/. Accessed 16 Feb 2023
33. What on earth is Blockchain?. https://timesofmalta.com/articles/view/What-on-earth-is-Blockchain.675774. Accessed 16 May 2023

Block-Privacy: Privacy Preserving Smart Healthcare Framework: Leveraging Blockchain and Functional Encryption

Bhaskara Santhosh Egala[1], Ashok Kumar Pradhan[1](✉), and Shubham Gupta[2]

[1] SRM University, Amaravati, Andhra Pradesh, India
[2] 3GPP NTN Researcher, Sateliot, Barcelona, Spain
{bhaskara_santhosh,ashokkumar.p}@srmap.edu.in

Abstract. Early adoption of Internet of Medical Things (IoMT) are enhancing the healthcare sector in all directions. Though the advances are adding advantages to the existing systems, the security and privacy of medical data remain a challenge. The increase in IoMT and mobile healthcare devices presence on untrusted networks can make the situation more complicated for healthcare system users. Moreover, they are pushing critical data to centralized locations like cloud, where the patient lacking control on his data. In this regard, a secure IoT framework is desirable which is capable of preserving the integrity and confidentiality of the medical data. Due to this, we proposed a novel architecture which leverages blockchain, IPFS, zero-knowledge protocols, and functional encryption technologies to provide decentralised healthcare system privacy and security. The proposed system helps the healthcare system administrators maintain data confidentiality, availability, integrity, and transparency over an untrusted peer-to-peer network without any human interference. Moreover, the system eliminates the requirement for a centralised server for functional encryption operations using hybrid computing paradigms. Finally, the proposed system suggests a novel mechanism to minimise the latency in data sharing over the network without compromising data security and privacy. To describe the working principle of this architecture a logical analysis is carried out which shows that the system is capable of providing the desired security and privacy.

Keywords: Blockchain · Security and Privacy · Functional Encryption · Zero-knowledge proof · Smart Healthcare · Internet of Medical Things (IoMT)

1 Introduction

Medical data privacy is a paramount concern in contemporary healthcare, given the sensitive nature of personal health information. The proliferation

D. Puthal et al. (Eds.): IFIPIoT 2023, IFIP AICT 684, pp. 114–132, 2024.
https://doi.org/10.1007/978-3-031-45882-8_9

of electronic health records (EHRs) and the sharing of data among healthcare stakeholders necessitate secure and privacy-preserving approaches to handle medical data [1]. Privacy breaches can have severe consequences, including discrimination, identity theft, and damage to a patient's reputation. Moreover, such breaches can erode trust in the healthcare system, leading patients to hesitate when disclosing personal information to their healthcare providers. Recent incidents like the AccuDoc Solutions breach highlight the significance of this issue [2]. With the advent of insecure internet technologies like IoMT, IoT, and CPS, ensuring the privacy and security of patient medical data has become an urgent matter. Additionally, managing and controlling access to generated data pose new challenges in smart healthcare systems. Any compromise of critical data can result in misconduct and loss of privacy. Traditional systems fall short in terms of data privacy, a fundamental requirement for the success of a healthcare system. Furthermore, medical records are typically stored and processed on cloud computing platforms, where data security and privacy are governed by third-party service providers. However, relying on centralized systems introduces uncertainty and limitations, and retrieving data from a centralized cloud is time-consuming and demands substantial bandwidth and a persistent connection. Moreover, factors such as transparency, scalability, traceability, user control, and integrity must be considered when designing a smart healthcare system framework.

To tackle these challenges, promising technologies such as blockchain, IPFS, hybrid computing paradigms, and privacy-preserving techniques of the new generation can be harnessed. Blockchain technology, with its tamper-proof public ledgers and smart contracts, contributes to data integrity and transparency [3]. Nevertheless, blockchain technology faces constraints regarding the storage and scalability of large-scale medical data, making it a costly option for sharing and storing sizable files. To address these challenges, we have explored the utilization of the InterPlanetary File System (IPFS), a decentralized file-sharing protocol built on blockchain technology. Additionally, we have employed edge computing to minimize latency by performing critical medical data processing at the network edge. This approach enables local data analysis and real-time decision-making [4]. Our proposed architecture also tackles resource limitations at IoT nodes by offloading complex operations to high-end devices. The traceability of actions and records is facilitated through IPFS on a private blockchain and an internal gateway. Smart contracts on the blockchain reduce transaction costs by eliminating the need for third-party involvement. IPFS provides a user-friendly web interface for sharing medical records on a peer-to-peer blockchain network, while edge computing offers real-time data analysis capabilities for critical situations, ensuring reduced latency. Cryptographic mechanisms enable user-controlled sharing of records, while cloud computing serves as the backbone network for the entire architecture, supporting remote patient monitoring. In the classical system, identity validation exposes confidential information to the verifier, which may result in privacy breaches. To ensure privacy-preserving identity validation, Zero-knowledge proofs are considered the optimal solution.

Zero-knowledge proofs offer an efficient mechanism for privacy protection, allowing one party to verify the truth of a statement declared by another party without revealing any raw data or relying on a third party [5]. The process of zero-knowledge proofs involves two primary roles: the prover, who generates a proof using raw data to validate the statement, and the verifier, who verifies the authenticity of the proof. Zero-knowledge proofs are widely employed in privacy-preserving schemes due to their completeness, soundness, and zero-knowledge property [6]. Completeness ensures that the truthfulness of the statement can be confirmed, while soundness guarantees that the prover cannot deceive the verifier with a false proof. Zero-knowledge ensures that the raw data remains confidential, enabling the prover to maintain ownership of the raw data during the proving and verifying processes to protect privacy. To facilitate the development of corresponding systems in real-world applications, a toolkit based on zero-knowledge succinct non-interactive arguments of knowledge (zkSNARK) has been introduced [7]. The zkSNARK toolkit allows the prover to prove its statement using a simple message with low computational complexity. A zkSNARK-based toolkit provides a flexible and efficient approach to creating a smart contract for automatic verification and generating the proof with raw data based on the specific application scenario.

Within this framework, the Selective Ring-Based Access Control (SRAC) [8] ensures data privacy during sharing. However, in certain cases, complete data is not required for analytics. In such scenarios, functional encryption is applied. Functional encryption is a form of encryption that enables a user to perform specific computations on encrypted data without accessing the actual data. Unlike traditional encryption, where the encrypted data is only accessible to those with the decryption key, functional encryption allows data to be encrypted based on specific attributes, such as a user's role or job title, and only users with the relevant attributes can decrypt the data. This approach offers several advantages over traditional encryption methods, which often necessitate decrypting the data before performing any computations. With functional encryption, the data remains encrypted throughout the computation process, reducing the risk of data breaches or unauthorized access.

In this paper, we present a comprehensive framework that integrates IoT, edge computing, blockchain, IPFS, gateways, and cloud computing to establish a healthcare monitoring system that ensures data security, privacy, traceability, transparency, user control, anonymity, and scalability. Our proposed system employs ECC-based cryptography modules to uphold confidentiality and privacy between the IoT layer and the edge layer. Patient registration IDs combined with edge computing and an IPFS file manager guarantee medical record anonymity. The system automates primary-level healthcare activities using smart contracts while offering enhanced control over medical data sharing with patients through functional encryption and zero-knowledge protocols. Additionally, the proposed system stores hash values of every medical record and critical event logs on the blockchain to prevent record forgery and improve medical services by providing accurate information and service alerts.

1.1 Research Problems, Challenges and Novel Contributions of the Current Paper

Research Problems:

i) The existing healthcare delivery systems are centralised. Lacks a centralised platform for the exchange of data and services between service providers.
ii) Traditional systems rely on centralised security management services provided by a third party, where data security and privacy remain ambiguous.
iii) Classical systems are dependent on static privacy and security management procedures, which restricts the system's ability to operate dynamically.

Challenges in Solving the Problems:

i) Decentralised distributed systems are complicated and challenging to build and operate.
ii) Establishing system-level privacy and security mechanisms with transparency, traceability, scalability, and availability is challenging.
iii) It is difficult and time-consuming to establish dynamic nature with several intra-privacy and security sub-modules.

Novel Contributions of the Current Paper:

i) A novel four-layer hybrid computing smart healthcare architecture introduced to address medical data security and privacy.
ii) A Blockchain-based zero-knowledge identity management fabricated with existing SRAC to enhance privacy and security capabilities.
iii) A ABE-FE based encrypted applyed on public DDSS to allow limited operations on encrypted data without compromising data privacy.
iv) Subsequently, A systematic security analysis presented by highlighting the benefits of the proposed architecture over classical healthcare systems.

The remaining sections of this paper are structured as follows: In Sect. 2, we review the related works and their contributions to the field of medical data privacy and security. Section 3 introduces the proposed system architecture and its mechanisms, including FE and Zokrates. In Sect. 4, we conduct a comprehensive analysis of the proposed system, including its performance and security aspects. Finally, we summarize the main contributions of this paper and discuss potential future work in Sect. 5.

2 Related Work

In this section, we present a literature review of the related work on different elements of the proposed smart healthcare system to showcase current trends.

One of the trending areas in the healthcare sector is the Internet of Medical Things (IoMT), which involves the use of wireless body area networks (WBAN) for patient monitoring. In [9], the authors discussed the latest trends in the field of IoMT and presented a patient monitoring system prototype based on WBAN. Another study on WBAN [10] utilised blockchain and IPFS to address transparency and traceability issues. Similarly, [11] presented an IoMT-based healthcare system model that focuses on patient monitoring and medical record management. To improve the scalability, traceability, and transparency of healthcare systems, various blockchain-based solutions have been proposed in [12,13]. For instance, in [12], a privacy-preserving scheme based on blockchain and cryptographic encryption techniques was proposed, while [13] suggested a medical system to verify patient medical data integrity and authenticity at the edge system level.

As blockchain data storage limitations pose a challenge to storing large amounts of data, researchers have proposed various solutions to overcome this problem. For example, a modified version of IPFS with Ethereum smart contracts was proposed in [15] to address this issue. Similarly, [16] introduced an edge-based blockchain model for secure medical data transmission, but the operational cost for continuous sensor data was high. In [17], a secure medical data-sharing framework was suggested using edge and blockchain platforms to reduce latency and cost. However, their work was limited to data sharing and access control. To address security and privacy issues of data offloading, [18] proposed a decentralised computing paradigm that offloads data sharing and communication. Furthermore, in [19], the authors introduced the concept of a private encrypted database, demonstrating that their approach satisfies ϵ-differential privacy in the continual observation model. They utilised structured encryption techniques [20] to develop a private histogram query scheme, which is a generalisation of symmetric searchable encryption. Based on this foundation, our study aims to explore the promising research directions in the emerging area of private encrypted databases. A Blockchain-based medical data-sharing framework, GlobeChain [21], is introduced to address centralized data exchange vulnerabilities and handle outbreak records. The article discusses potential challenges and future directions for the proposed Blockchain-based framework's effectiveness. A unified Blockchain-based model to connect different e-health systems seamlessly, ensuring access to large-scale patient data without significant modifications, while also addressing security and privacy concerns is presented in [22].

Zero-knowledge proofs are widely used to ensure privacy in various domains, including the cryptocurrency field. For example, Zcash implemented a privacy-protected digital currency system using zero-knowledge proofs. In [23], Eberhardt combined zero-knowledge proofs with an Ethereum smart contract by designing ZoKrates, a zero-knowledge proof mode of offline computing and online verification. This has expanded the possible applications of zero-knowledge proofs. Westerkamp [24] proposed a side chain-proof mechanism using ZoKrates, while Ibrahem [25] applied zero-knowledge proofs and homomorphic encryption to an anonymous voting system. In the Internet of Vehicles domain, Rasheed et al. [26] implemented an anonymity authentication method based on zero-knowledge proofs, while Jeong et al. [27] used smart contracts and zero-knowledge proofs in online real-estate transactions to provide a transaction process with a privacy protection mechanism. In [28], Qi et al. applied zero-knowledge proofs to the auto insurance industry to achieve an effective insurance evaluation method based on habits while preserving privacy. Umar et al. [29] have combined zero-knowledge proofs with wireless body sensors to effectively avoid privacy leakage caused by malicious attackers monitoring communication channels. It is feasible and beneficial to apply zero-knowledge proofs to the privacy protection process of production data traceability.

3 System Architecture

In this section, we present our proposed smart healthcare framework called "Block-Privacy," consisting of four computing layers, as illustrated in Fig. 1. The architecture we propose ensures system-level privacy, security, and transparency through the integration of distributed decentralized storage systems (DDSS), zero-knowledge proof identity validation, and functional encryption (FE). To establish traceability, all critical events and patient medical data at the system level are stored in DDSS. To mitigate potential downtime or data unavailability, our system incorporates Byzantine fault tolerance, employing IPFS cache and off-chain storage. The respective layers within our system synchronize their data with the DDSS network, thereby increasing data availability. Off-chain cache management introduces redundancy, but requests and responses are based solely on active data from the edge layer or the fog layer. Selective ring-based access control (SRAC) utilizes blockchain-based smart contracts to generate and update the access rule table on DDSS. Furthermore, we enhance real-time transparency through the use of private blockchain and IPFS, while smart contracts automate the actions of actuators and facilitate tamper-proof digital agreements among stakeholders. To ensure secure communication between nodes, we adopt the DTLS protocol, complemented by public key cryptography, thereby guaranteeing data confidentiality. The initial step in the proposed system involves actor and node registration, which sets the foundation for system operations. Pseudo registration IDs are created to ensure system-level anonymity and facilitate future identification. For each actor, the system generates two distinct and mathematically related numbers: a private ID and a public ID. The private ID is exclusively shared with DDSS at the edge and fog computing layers to enable anonymous management of medical data records. Conversely, sensors are intentionally assigned public IDs and service identifiers to facilitate data generation.

Moreover, the private ID, serving as the patient's directory name, is utilized for storing records in the IPFS local manager. Hybrid computing plays a pivotal role in simultaneous data processing, analysis, and decision-making. To avoid confusion in medical treatments, IPFS retains record versions, while the hash value of each medical record is published on the blockchain to ensure traceability and transparency. The local IPFS file manager is responsible for managing patient records within the hospital, while cloud-based IPFS systems handle patient data beyond the hospital premises. Specific requests for patient records

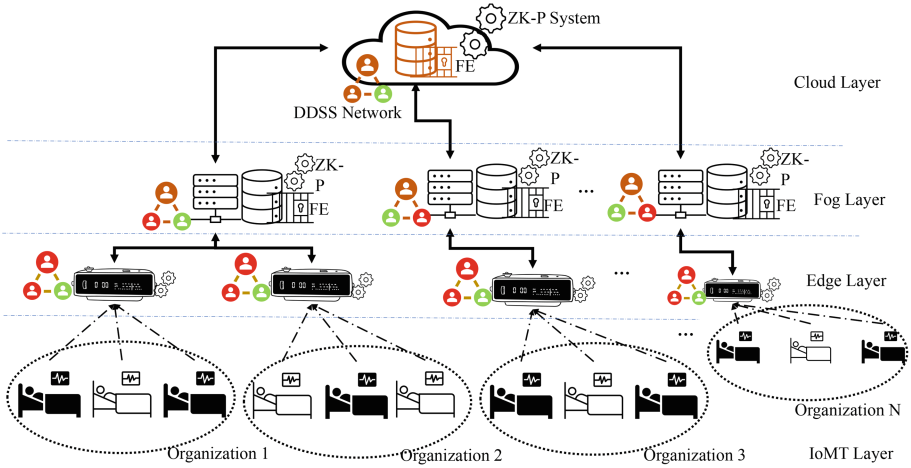


Fig. 1. Proposed system architecture in layered view

are redirected to the nearby IPFS module for local caching. If the requested medical record is not available in the local cache, the request is forwarded to the global IPFS module. When a request reaches the hybrid computing layer, patient IDs are mapped to corresponding records, which are then encrypted using an ECDH secret key. To ensure uninterrupted data accessibility, the IPFS module maintains mirror copies of each medical record at both the edge computing and cloud computing levels. Smart contracts facilitate digital agreements between other stakeholders and the patient for services provided outside the hospital, while also generating service-based alerts that are sent to patients and their nominees. The internal computing layers of the proposed model are further elucidated as follows:

3.1 IoMT Layer

The IoMT layer consists of medical sensors (S) and actuators (A). In the proposed system, medical services through the IoMT devices are performed using logical groups with a unique service tag ST_{Pid}. As shown in the system architecture, every hospital (organisation) has its own virtual boundaries with a unique organisation identity ID_{Org}. Every device in this layer generates the patient's medical data (MD_{Pid}) in real-time. The generated MD_{pid} is published to the near-by edge device in encrypted format using an ECC-160-bit edge public key (KY_{Edg}). Additionally, a hash of data (HC_S) and device identity token (IT_{Div}) are added for authentication and data integrity validation. At this layer, devices are limited to performing only three operations: registration, authentication, and transferring medical data. Other than these limited compulsory actions, devices are not allowed to participate in any system-level operations to preserve the limited device resources and device integrity. In the device registration process, the edge computer acts as the verifier and registering authority. In order to register with a nearby edge computer, the IoMT device sends the joining request (Rq_{Join}) on its local service region network (i.e., a hospital). The request contains a 32-bit string concatenated with an 8bit-size random number (RN_{Join}). The string contains the device pseudo identity ($PsID_{Div}$), location code (CD_{Loc}), and ST_{Pid}. Upon receiving the request, the edge computer validates the request by checking the information on DDSS. When the requested device information is true, the edge computer generates an operational identity (ID_{Opr}) for the device using $PsID_{Div}$ and RN_{Join}. To generate ID_{Opr}, edge computer generates one random number (RnE_{temp}) and computes ID_{Opr} = Hash($RN_{Join}{}^{RnE_{temp}}$), also saving $Hash(ID_{Opr})$ on DDSS. This ID_{Opr} is encrypted with RN_{Join} and handed over to the requester. The ID_{Opr}, ST_{Pid} and ID_{Org} are used by the device for patient services. In order to rejoin, the device sends a rejoin request (which contains $Hash(ID_{Opr})$). The MD_{Pid} is encrypted with KY_{Edg} named based on the patient pseudo identity for DDSS version control.

3.2 Edge Layer

In this layer, the edge computer takes care of local data processing and segregation and secure storage on DDSS. In the first place, the edge computer is to register using a join request. The request is broadcast on the local DDSS network, represented by a red network symbol in the system architecture. The green icon indicates the underlined IPFS peer-to-peer network. Another red icon indicates the DDSS network between edge and fog layers. Based on the one-third approval request, the requester is listed in the table and marked as authorised. In order to rejoin, no poling is conducted; instead, a blockchain-based Zokrates zero-knowledge proof is used for identity validation with a high level of privacy. The working model of Zokrates is explained in Sect. 3.5. All these communications are encrypted with the layer public key (KY_{EdL}).

The edge computer decrypts the received MD_{Pid} and validates its integrity before conducting data analytics on it. Assuming that the data is not modified in the communication and that the meta information of the data (i.e. ID_{Org}, ST_{Pid} and $Hash(ID_{Opr})$) is genuine, the data is encrypted and published to the next-level DDSS layer. Until this layer, the access control rules are applied using the selective ring-based access control system (SRAC) [8]. It handles the most critical activities like $DataProcessing()$, $DataAnalysis()$, $DecisionMaking()$ for automatic medical activities. Simultaneously, it sends alerts using $Alert()$ to caretakers and doctors in emergencies and sends actions to actuators using Smart Contracts.

3.3 Fog Layer

The fog layer provides fog computing services to the proposed system framework. It acts as the main DDSS network-based storage and computing platform for the edge layer. Every edge computer publishes their segregated data based on individual patients on the DDSS network (i.e., between the edge and fog layers) using FE and SRAC. Fog nodes also follow the same device registration and identity validation mechanisms as the edge layer. In addition to ZK-P, this layer provides FE services for the highest level of privacy without limiting the availability of data for analysis. The edge-to-fog layer device identity validation is achieved without sharing any confidential data with the help of Zokrates mechanism. In this layer, off-chain secure data backups are created with the layer's public key (KY_{PuF}). This layer acts as the live network for the system requirements, where the rules, data, and network updates are frequent and synchronised in real-time. All community-based data requests and analyses are handled by fog layer computing.

3.4 Cloud Layer

The top layer, or upper layer, in the proposed layer is the cloud layer, where limited global-level data analyses using FE are allowed. Moreover, it acts as a global-level data provider and meta-information provider. In this layer, no SRAC mechanism is allowed; only FE functional operations are allowed, and no access to complete data is guaranteed with the encryption function $f()$ and secret key of that function KY_{SF}. Due to its high scalability and low cost, this layer is used in emergencies or on a need-basis for high-level functional operations. The edge and fog layers are connected using a global-level DDSS network. Where the updates are scheduled at long intervals.

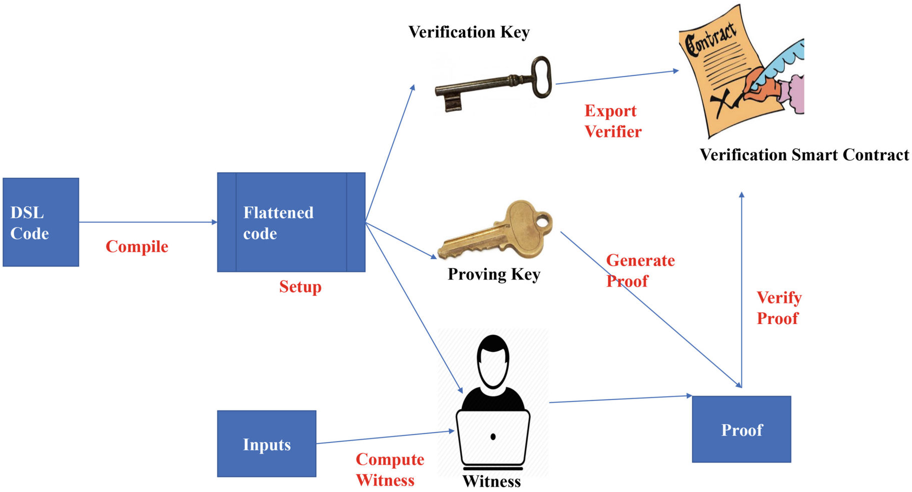


Fig. 2. The Zokrates proof setup

3.5 Data Security and Privacy Mechanisms

The proposed system has three cryptographic mechanisms for data privacy and security. The first one is SRAC for data sharing between authorised actors. SRAC is a blockchain-based, lightweight access control system that guarantees better throughput. The second one is Zokrates zero-knowledge proof-based identity validation, and the final one is FE based on optimal data privacy in data analytics.

3.5.1 Zokrates Identity Validation: To integrate Zokrates in black-box mode, we have executed a series of systematic steps, as illustrated in Fig. 2. In this section, we present a detailed account of the steps undertaken to successfully establish Zokrates in black-box mode. When a prover wants to demonstrate their knowledge of the calculation result z, they will construct a proof using the corresponding proving key, together with the public inputs x and the private input w. Following this, the verifier will employ the appropriate verifier key, the public inputs x, and the proof presented by the prover to verify and certify the correctness of the computation's output.

i) **Define the Program:** The first step is to define the program that will be used for the ZKP. This program should take as input the values that the prover knows and produce as output some computation on those values.
ii) **Compile the Program:** A series of arithmetic circuits, which are simply mathematical equations that reflect the calculation of the program, are created once the software has been constructed.
iii) **Generate the Witness:** The input values and intermediate values that are created throughout the computation are combined to create a witness by the prover.
iv) **Compute the Proof:** The prover computes a proof of knowledge-a mathematical demonstration-using the witness that they are aware of the input values without disclosing them.
v) **Verify the Proof:** Upon receipt of the proof, the verifier engages in a validation process utilizing arithmetic circuits. Crucially, the verifier can assess the proof's validity while maintaining a strict ignorance regarding the input values and the witness itself.

The zero-knowledge proof process entails represented with symbolic notation. Initially, random values are generated for $\alpha, \beta, \gamma, \delta,$ x and the set τ and σ are generated with the cyclic subgroup Fr of the elliptic curve. Whereas $\alpha, \beta, \gamma,$ and δ are polynomials, while x is a randomly chosen number.

$$\tau = (\alpha, \beta, \gamma, \delta, x)$$

(1)

$$\sigma = ([\sigma_1]_1 , [\sigma_2]_2)$$

(2)

$$\sigma_1 = \left(\alpha, \beta, \delta \left\{x^i\right\} \{i = 0 \wedge n-1\} , \left\{\left(\frac{\beta u_i(x) + \alpha v_i(x) + w_i(x)}{p}\right)\right\}_{i=0\wedge 1} , \left\{\frac{\beta u_i(x) + \alpha v_i(x) + w_i(x)}{\delta}\right\}_{i=1+1}^{\wedge m} , \left\{\frac{x^i t(x)}{\delta}\right\}_{i=0\wedge n-2}\right)$$

(3)

$$\sigma_2 = \left(\beta, \gamma, \delta \left\{x^i\right\}_{i=0\wedge n-1}\right)$$

(4)

The process of generating the proof is to randomly select two parameters r and s, calculate $\pi = \varPi\sigma = ([A]_1, [C]_1, [B]_2)$. Among them: $A = \alpha + \varSigma_{i=0-m}\alpha_i u_i(x) + r\delta$, $B = \beta + \varSigma_{i=0-m}\alpha_i u_i(x) + s\delta$, and $C = \{\varSigma_{i=1+1-m} a_i \left(\beta u_i(x) + \alpha v_i(x) + w_i(x)\right) + h(x)t(x)\} / \{\delta\} + As + rB - rs\delta$

At present, system generates the three points on the elliptic curve, the B needs to be calculated twice. At the same time $H(x)$ is calculated with the quadratic arithmetic program (QAP equation). Later, points are handed over to the verifier for verification. The verification formula is: $A\cdot$B$= \alpha \cdot \beta + \{\varSigma_{i=0-1} a_i \left(\beta u_i(x) + \alpha v_i(x) + w_i(x)\right)\} / \{\gamma\} \cdot \gamma + C \cdot \delta$

Therefore, the perfect zero-knowledge of the algorithm can be verified by the following formula:

$C = \left(AB - \alpha\beta - \varSigma_{i=0-1} a_i \left(\beta u_i(x) + \alpha v_i(x) + w_i(x)\right)\right) / \delta.$

We only need to prove that in the case of providing τ and public key $(a_0, a_1, \ldots, a_1)$, a verifiable proof π can be obtained through calculation even if the private key information $(a_{1+1}, a_{1+2}, \ldots, a_m)$ is not known.A transaction consists of points A, B, C along with *input* values as show in Fig. 3. Moreover, it showcases the chosen scheme and curve where the system works.

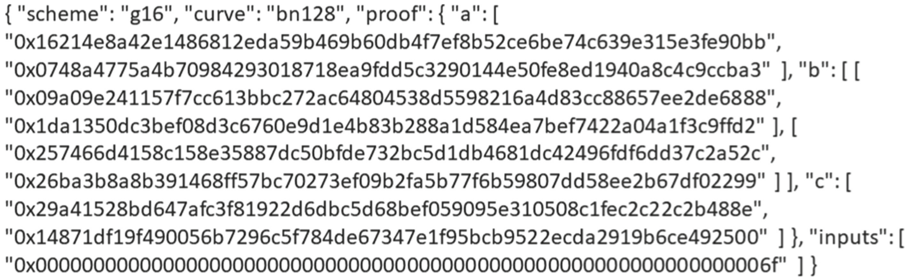

{ "scheme": "g16", "curve": "bn128", "proof": { "a": [
"0x16214e8a42e1486812eda59b469b60db4f7ef8b52ce6be74c639e315e3fe90bb",
"0x0748a4775a4b70984293018718ea9fdd5c3290144e50fe8ed1940a8c4c9ccba3"], "b": [[
"0x09a09e241157f7cc613bbc272ac64804538d5598216a4d83cc88657ee2de6888",
"0x1da1350dc3bef08d3c6760e9d1e4b83b288a1d584ea7bef7422a04a1f3c9ffd2"], [
"0x257466d4158c158e35887dc50bfde732bc5d1db4681dc42496fdf6dd37c2a52c",
"0x26ba3b8a8b391468ff57bc70273ef09b2fa5b77f6b59807dd58ee2b67df02299"]], "c": [
"0x29a41528bd647afc3f81922d6dbc5d68bef059095e310508c1fec2c22c2b488e",
"0x14871df19f490056b7296c5f784de67347e1f95bcb9522ecda2919b6ce492500"] }, "inputs": [
"0x000000000000000000000000000000000000000000000000000000000000006f"] }

Fig. 3. Zokrates Transaction Details

3.5.2 Functional Encryption Operations: To ensure robust data privacy in data analytics, we have incorporated attribute-based functional encryption (ABE) as depicted in Fig. 4. In this section, we outline the experimental steps undertaken to illustrate the implementation and efficacy of ABE-based functional encryption.

i) **Key Generation:** Given a security parameter λ, the attribute authority generates a master secret key (msk) and a set of public parameters (params). Each user U is assigned a set of attributes Attr(U).
ii) **Encryption:** To encrypt a message m with attributes Attr(m), we run the encryption algorithm Enc(params, m, Attr(m)) which outputs a ciphertext C. Enc(params, m, Attr(m)) = (pk, C), where pk is the public key and C is the ciphertext.
iii) **Decryption:** To decrypt a ciphertext C with attributes Attr(C), a user U with attributes Attr(U) provides a decryption key K_U

that is associated with a function G_U. The decryption algorithm $Dec(msk, K_U, C, Attr(C))$ outputs $G_U(Attr(U), m)$, where m is the decrypted plaintext. $Dec(msk, K_U, C, Attr(C)) = G_U(Attr(U), m)$, where m is the decrypted plaintext.

iv) **Function Generation:** To generate a decryption key K_U for a user U that is associated with a function G_U, we run the function generation algorithm $Gen(msk, Attr(U), G_U)$, which outputs the decryption key K_U. $Gen(msk, Attr(U), G_U) = K_U$, where K_U is the decryption key associated with the function G_U as shown in Fig. 5.

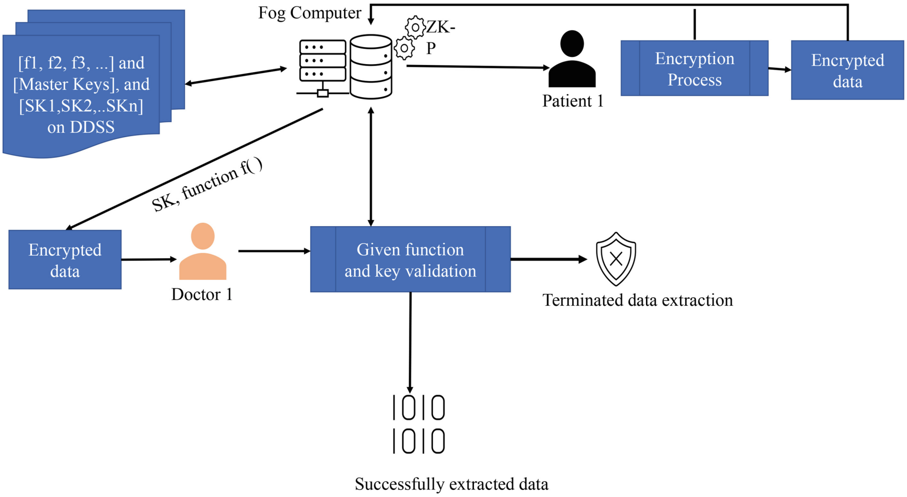


Fig. 4. The Flow diagram of FE in proposed system

Use-case: In our proposed system, the fog node employs functional encryption to encrypt data m using two attributes: $A1$ representing the patient's age and $A2$ representing the patient's medical history. The encryption process involves the generation of a function F that takes the attributes and data as input and produces attributes and ciphertext as output, as illustrated by $F(A1, A2, m) = (A1, A2, c)$. Subsequently, decryption keys are generated for each authenticated user using the function G. For example, for doctor1 with attributes (A1≥50), a decryption key $d1$ is generated using $G1(A1, m) =$ "The patient has high blood pressure and is over 50 years old." In another scenario, for a different doctor, a decryption key $d2$ is generated as follows: $G2(A2, m) =$ "The patient has high blood pressure and a heart condition." When a doctor with attributes (A1≥50) intends to decrypt the message m, they must provide $d1$, $A1$, and $A2$. The decryption algorithm searches for matching conditions, such as A1≥50, within the encrypted message. Upon identifying a match, the decryption function is applied to obtain the original message. This approach ensures that only authorized users with the appropriate attributes can access

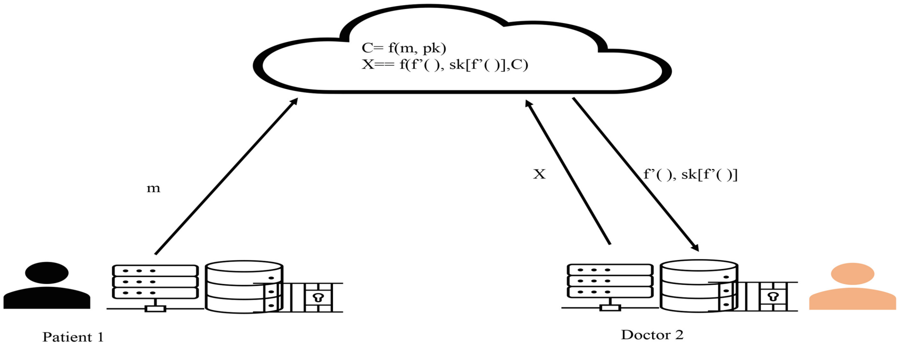


Fig. 5. In the context of patient1's data, doctor 1 aims to execute a specific operation denoted as f. To facilitate this, the doctor shares both the function f itself and the corresponding secret key $sk[f]$ with patient1. Subsequently, patient1 encrypts the data m and shares the resulting encrypted version, denoted as c, with doctor 1. Leveraging the provided secret key $sk[f]$, doctor 1 proceeds to decrypt the encrypted data c and perform the desired operation f on m, yielding the outcome $f(m)$.

the encrypted data, providing a fine-grained level of access control while preserving data privacy and confidentiality.

4 Systems Analysis

The present study introduces an advanced healthcare monitoring system that employs cutting-edge technologies to provide enhanced privacy functionalities when compared to conventional systems. This section aims to thoroughly analyze the security and privacy aspects of Block-Privacy. Furthermore, we assess the unique characteristics offered by our proposed system. For the computational analysis of FE and ZK-P, we utilized a Windows operating system equipped with an Intel i5-H CPU running at a frequency of 2.5GHz, accompanied by 16GB of RAM and a 4GB GPU. Conversely, the DDSS system analysis was conducted on an Ubuntu system with 8GB of RAM and an Intel i5-H CPU. To achieve the desired outcomes, we employed proof-of-stack (PoS) for DDSS and proof-of-work (PoW) for ZK-P.

Security: In order to ensure secure communication across the IoMT-edge-Fog layers, all transmissions are encrypted utilizing the respective layer's public key. Internally, messages are encrypted using the public keys of the intended recipients. The DDSS system hosts all the necessary keys at various layers. To maintain data integrity, a comprehensive validation process is conducted at each stage of data processing and storage. Once the data has been written to the DDSS blockchain, any unauthorized modification of the data is effectively prevented. The availability of medical data is guaranteed at every layer. In the IoMT layer nodes, real-time patient service is facilitated by allocating idle nodes. For the remaining layers, data availability is ensured through the utilization of off-chain storage, Byzantine fault tolerance, and the IPFS cache. To safeguard data confidentiality at multiple levels, robust encryption techniques such as the ECC-ecosystem are employed.

Privacy: In the present study, the privacy of medical records is ensured through the utilization of FE-based encryption and SRAC. The encrypted data can only be functionally operated upon by authorized parties without the need for plain information sharing. The ZK-P technology allows participating actors to verify their identity while preventing the disclosure of confidential information. Moreover, sensitive or critical data residing in the edge layer (local DDSS) is segregated and only accessible through edge computing. Physical and digital access control mechanisms are employed to ensure the perpetual protection of this data.

Transparency: The function $AddToBlockchain()$ serves the purpose of appending blocks to the chain. The blockchain engine, being devoid of any centralized authority, ensures transparency in the maintenance of medical records. The utilization of immutable ledgers within the blockchain framework facilitates the resolution of disputes between patients and healthcare professionals by providing a comprehensive record of actions undertaken.

Immutability: The blockchain-based DDSS and ZK-P systems demonstrate immutability, as once a transaction is approved, it becomes unalterable and irremovable from the DDSS ledger. This stands in contrast to traditional systems, where data is susceptible to inadvertent or malevolent modifications.

Anonymity: The ZK-P mechanism introduces a noteworthy enhancement in identity validation by eliminating the need for identity revelation. Instead, identity validation relies solely on challenge and response codes. This innovative approach ensures that the original device identity remains concealed from the verifier, thus establishing a desirable level of anonymity within the proposed system. Furthermore, the patient's data is stored on DDSS utilizing a pseudo identity, further protecting their true identity. Service monitoring is facilitated through the utilization of service tags, rather than patient identities, adding an additional layer of privacy and confidentiality.

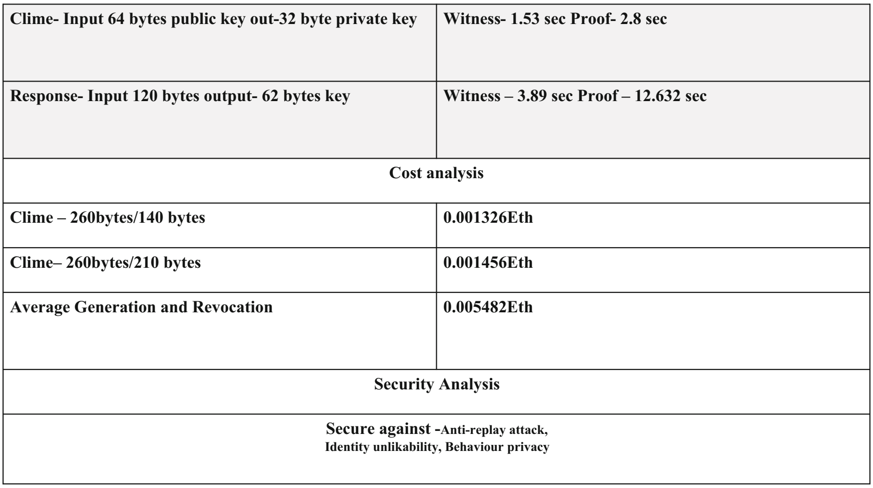
User-Control: The suggested approach enables SRAC and FE control of the data by the data owner. In a traditional system, healthcare providers are in charge of data.

Scalability: Given the inherent scaling challenges associated with blockchain technology, the proposed system addresses this issue by incorporating IPFS as an auxiliary technology, effectively mitigating storage concerns. The data is published to IPFS, and its tracking is accomplished through a blockchain ledger utilizing DDSS methods. This synergistic approach ensures efficient and effective data management. Furthermore, the proposed system empowers users with the ability to selectively share either comprehensive datasets or specific pieces of information in accordance with their preferences and requirements.

4.1 Cost Analysis

In order to assess the performance of our system, a comparative analysis was conducted, taking into account various aspects such as bandwidth cost, resource consumption, blockchain data storage cost, and cryptography overhead on nodes. The findings of this evaluation are summarized in Table 1, showcasing the cost and throughput analysis of the proposed system utilizing ZK-P. Notably, the system demonstrated efficient processing times of 1.53 s and 2.8 s for witness and proof generation, respectively, with a claim size of 64 bytes and an output private key of 32 bytes. Additionally, for a claim size of 260 bytes and an output key of 140 bytes, the system consumed a mere 0.001326 ether. These results unequivocally indicate the feasibility of implementing real-time identity validation within the proposed system.

Table 1. Cost and Throughput analysis



Clime- Input 64 bytes public key out-32 byte private key	**Witness- 1.53 sec Proof- 2.8 sec**
Response- Input 120 bytes output- 62 bytes key	**Witness – 3.89 sec Proof – 12.632 sec**
Cost analysis	
Clime – 260bytes/140 bytes	**0.001326Eth**
Clime– 260bytes/210 bytes	**0.001456Eth**
Average Generation and Revocation	**0.005482Eth**
Security Analysis	
Secure against -Anti-replay attack, Identity unlikability, Behaviour privacy	

Performance and Bandwidth Cost: Conventional systems rely on central cloud computing to handle and process data. However, this approach entails several drawbacks, including exorbitant bandwidth costs, constant reliance on cloud connectivity, and data availability being contingent upon the efficiency of communication channels. In contrast, our system embraces a hybrid computing paradigm, harnessing the advantages of small bandwidth requirements. The performance of our system does bear some dependence on the effectiveness of communication channels. Functional operations on encrypted data with DDSS cache support are presented in Table 2. Time intervals are measured in seconds. The process of extracting 60 bytes of data from DDSS utilizing FE required a duration of 0.78 s. For 120 bytes, it took 1.81 s, and for 240 bytes, it took 3.2 s. Although the current operational time intervals exhibit some slowness, future efforts can be directed towards optimizing the functions to expedite the overall process. To evaluate the performance of the proposed system, various metrics were considered, including transactions per second (TPS). The TPS analysis involved performing one hundred operations for registration, quarrying, and update status on the distributed decentralized storage systems (DDSS) with three concurrent connections from three nodes. The system consumed an average latency of 1.04 s for registration identification, 1.23 s for query identification, and 1.06 s for status updates, respectively. The throughput of the system varies for each action, as detailed in Table 3. Despite the system's complex structure, spanning across four layers of computing framework, it demonstrates satisfactory performance levels.

Table 2. FE functional operations on DDSS data

Size	Key Generation	Encryption	Decryption	Total Time
60 bytes	0.28	0.37	0.41	0.78
120 bytes	0.6	0.81	1	1.81
240 bytes	1.2	1.5	1.8	3.2

Table 3. DDSS Performance with SRAC

Operation	Max Latency (s)	Min Latency (s)	Avg Latency (s)	Throughput (TPS)
Register identity	2.6	0.075	1.04	265.2
Query identity	2.2	0.24	1.23	216
Update sautes	2.56	0.63	1.06	263

Resource Consumption: Traditional healthcare systems rely on central cloud computing, which is a cost-effective option that enables real-time resource scaling. However, this approach provides a limited resource pool and insufficient real-time data processing and decision-making capabilities for handling critical healthcare activities. In future healthcare applications, real-time reactions will be required. Although our proposed model requires significant resources at the outset, it has the potential to revolutionize the use of healthcare applications in th future.

Blockchain Operational Overhead: While the IPFS protocol serves as a means to distribute files across a decentralized peer-to-peer network, the utilization of blockchain for file storage poses cost challenges. In the proposed system, medical records and critical events are uniquely identified on the blockchain solely by their hash values. The actual files, however, are stored either in local

IPFS storage or IPFS cloud storage. To ensure the utmost anonymity in device identity validation, the Zokrates-based approach is employed, thereby introducing additional costs to the already existing blockchain processes.

5 Conclusions and Future Work

Our proposed work presents a groundbreaking solution to address the multifaceted challenges concerning security, privacy, anonymity, and transparency of decentralized healthcare data. Furthermore, it effectively preserves valuable IoT resources by strategically transferring critical operations to the hybrid computing layer. Leveraging blockchain technology, our system ensures the establishment of tamper-proof public ledgers containing hash values of data and special event logs. The utilization of Zokrates proof guarantees secure identity validation without compromising the confidentiality of sensitive information during communication. Moreover, an attribute-based functional encryption mechanism safeguards against data leakage across cloud and intermediate nodes. Through comprehensive logical analysis, we have demonstrated that our system delivers the expected functionality in relation to the aforementioned concerns. Future endeavors encompass implementing intelligent data analysis on encrypted data and reducing system operation latency through the optimization of encryption functions and cryptographic operations.

References

1. Egala, B.S., Pradhan, A.K., Dey, P., Badarla, V., Mohanty, S.P.: Fortified-chain 2.0: intelligent blockchain for decentralized smart healthcare system. IEEE Internet Things J. **10**(14), 12308–12321 (2023). https://doi.org/10.1109/JIOT.2023.3247452
2. Davis, J.: 2.65M Atrium Health Patient Records Breached in Third-Party Vendor Hack. Health IT Security (2018). https://healthitsecurity.com/news/2.65m-atrium-health-patient-records-breached-in-third-party-vendor-hack
3. Hasavari, S., Song, Y.T.: A secure and scalable data source for emergency medical care using blockchain technology. In: 2019 IEEE 17th International Conference on Software Engineering Research, Management and Applications (SERA), Honolulu, pp. 71–75 (2019). https://doi.org/10.1109/SERA.2019.8886792
4. Egala, B.S., et al.: iBlock: an intelligent decentralised blockchain-based pandemic detection and assisting system. J. Sign. Process. Syst. **94**, 595–608 (2022). https://doi.org/10.1007/s11265-021-01704-9
5. Brandt, J., Damgard, I., Landrock, P., Pedersen, T.: Zeroknowledge authentication scheme with secret key exchange. J. Cryptol. **11**(3), 147–159 (1998)
6. Catalano, D., Visconti, I.: Hybrid commitments and their applications to zero-knowledge proof systems. Theor. Comput. Sci. **374**(1–3), 229–260 (2007)
7. Kim, J., Lee, J., Oh, H.: Simulation-extractable ZK-SNARK with a single verification. IEEE Access **8**, 156569 (2020)
8. Egala, B.S., Pradhan, A.K., Badarla, V., Mohanty, S.P.: Fortified-chain: a blockchain-based framework for security and privacy-assured internet of medical things with effective access control. IEEE Internet Things J. **8**(14), 11717–11731 (2021). https://doi.org/10.1109/JIOT.2021.3058946

9. Ahouandjinou, A.S.R.M., Assogba, K., Motamed, C.: Smart and pervasive ICU based-IoT for improving intensive health care. In: International Conference on Bio-engineering for Smart Technologies, pp. 285–292 (2016)
10. Shi, W., Cao, J., Zhang, Q., Li, Y., Xu, L.: Edge computing: vision and challenges. IEEE Internet Things J. **3**, 637–646 (2016)
11. Yuan, A., Mugen, P., Zhang, K.: Edge computing technologies for Internet of Things: a primer. Digit. Commun. Netw. **4**, 77–86 (2018)
12. Hayajneh, T., et al.: Secure authentication for remote patient monitoring with wireless medical sensor networks. Sensors **16**, 1–25 (2016)
13. Wang, S., et al.: Blockchain-powered parallel healthcare systems based on the ACP approach. IEEE Trans. Comput. Soc. Syst. **5**, 942–950 (2018)
14. Chen, et al.: A 5G cognitive system for healthcare. In: Big Data and Cognitive Computing, vol. 1, p. 2 (2017). https://doi.org/10.3390/bdcc1010002
15. Sicari, S., Rizzardi, A., Grieco, L.A., Coen-Porisini, A.: Security, privacy and trust in Internet of Things: the road ahead. Comput. Netw. **76**, 146–164 (2015)
16. Ranganathan, K., Iamnitchi, A., Foster, I.: Improving data availability through dynamic model-driven replication in large peer-to-peer communities. In: Proceedings of the 2nd IEEE/ACM International Symposium on Cluster Computing and the Grid (CCGRID'02), p. 376 (2002)
17. Shi, W., Cao, J., Zhang, Q., Li, Y., Xu, L.: Edge computing: vision and challenges. IEEE Internet Things J. **3**, 637–646 (2016)
18. Cyran, M.: Blockchain as a foundation for sharing healthcare data. Blockchain Healthc. Today (2018). https://doi.org/10.30953/bhty.v1.13
19. Agarwal, A., Herlihy, M., Kamara, S., Moataz, T.: Encrypted databases for differential privacy. Proc. Privacy Enhanc. Technol. **3**, 170–190 (2019)
20. Kamara, S., Moataz, T., Ohrimenko, O.: Structured encryption and leakage suppression. In: Shacham, H., Boldyreva, A. (eds.) CRYPTO 2018. LNCS, vol. 10991, pp. 339–370. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-96884-1_12
21. Biswas, S., Sharif, K., Li, F., Bairagi, A.K., Latif, Z., Mohanty, S.P.: GlobeChain: an interoperable blockchain for global sharing of healthcare data-a COVID-19 perspective. In: IEEE Consumer Electron. Magaz. **10**(5), 64–69 (2021). https://doi.org/10.1109/MCE.2021.3074688
22. Biswas, S., Sharif, K., Li, F., Alam, I., Mohanty, S.P.: DAAC: digital asset access control in a unified blockchain based E-health system. IEEE Trans. Big Data **8**(5), 1273–1287 (2022). https://doi.org/10.1109/TBDATA.2020.3037914
23. Eberhardt, J., Tai, S.: ZoKrates - scalable privacy-preserving off-chain computations. In: Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (2018)
24. Westerkamp, M., Eberhardt, J.: zkRelay: facilitating Sidechains using zkSNARK-based chain-relays. In: Proceedings of the IEEE Security and Privacy on the Blockchain (IEEE S&B 2020) (2020)
25. Ibrahem, M.K.: Robust Electronic Voting System Using Homomorphic Encryption Protocol and Zero-Knowledge Proof **5**(1) (2016)
26. Rasheed, A.A., Mahapatra, R.N., Lup, F.H.: Adaptive group-based zero knowledge proof-authentication Protocol (AGZKP-AP) in vehicular Ad-hoc networks. IEEE Trans. Intell. Transp. Syst. **21** (2019)
27. Jeong, S.H., Ahn, B.: Implementation of real estate contract system using zero knowledge proof algorithm based blockchain. J. Supercomput. **77**(10), 11881 (2021)

28. Qi, H., Wan, Z., Guan, Z., Cheng, X.: Scalable decentralized privacy-preserving usage-based insurance for vehicles. IEEE Internet Things J. **8**, 1 (2020)
29. Umar, M., Wu, Z., Liao, X.: Channel characteristics aware zero knowledge proof based authentication scheme in body area networks. Ad Hoc Netw. **112**(9), 102374 (2021)

zkHealthChain - Blockchain Enabled Supply Chain in Healthcare Using Zero Knowledge

G. Naga Nithin[1,2], Ashok Kumar Pradhan[1,2(✉)], and Gandharba Swain[1,2]

[1] SRM University, Amaravati, AP, India
ashokkumar.p@srmap.edu.in

[2] Department of Computer Science Engineering, KL University, Vaddeswaram, India

Abstract. Globalization has led to complex, cloud-centric supply chains that require transparency and traceability in the manufacturing process. However, traditional supply chain models are vulnerable to single points of failure and lack a people-centric approach. To address these challenges, our proposed work presents an innovative healthcare supply chain model that utilizes blockchain technology combined with Zero Knowledge Proofs (zk-SNARKs) and role-based access control (RBAC) mechanisms. The addition of RBAC to the proposed model ensures that only authorized users can access certain data and functionalities within the system, while improving the security and access control. This approach guarantees secure storage of business-sensitive data while enabling real-time product tracking and traceability. The proposed model was tested using an Ethereum-based decentralized application (DApp), demonstrating the preservation of digital record integrity, availability, and scalability by eliminating single points of failure. The system also offers privacy and security for sensitive data through the use of zk-SNARKs. In case of product faults, the model enables error tracing without disclosing the entire data set through the use of document hashes. By incorporating RBAC access control mechanisms, our proposed solution offers an effective, secure, and privacy-preserving mechanism for handling sensitive data, also benefiting stakeholders in the supply chain ecosystem.

Keywords: Blockchain · Zero Knowledge Proof · Access Control · Supply chain

1 Introduction

The healthcare industry is experiencing significant growth, with an estimated increase of 5% between 2017 and 2019, and projected to continue with an additional 6% in the next five years. The monitoring and management of the flow of medicines, medical products, and healthcare services from manufacturer to patient is critical to ensure that patients and healthcare professionals have access to the necessary treatments and medications. To address the challenges of data

D. Puthal et al. (Eds.): IFIPIoT 2023, IFIP AICT 684, pp. 133–148, 2024.
https://doi.org/10.1007/978-3-031-45882-8_10

silos and lack of transparency in the healthcare supply chain, innovative solutions are being developed. One such solution is the implementation of blockchain technology, which is a decentralized, unchangeable ledger that simplifies the storage of data and management of digital assets in a business network. It can automate transactions without human intervention, increasing efficiency and transparency.

However, as blockchain technology evolves, the issue of trust and privacy among users remains a concern. The use of traditional authentication methods such as passwords or private keys may not be sufficient to ensure the security of an individual's information as hacking becomes more sophisticated. Additionally, the transparency of blockchain technology can raise concerns about the privacy of sensitive and confidential data, as it is visible to all members of the network. To address these issues, the use of Zero Knowledge Proofs (ZKPs) is being explored in the healthcare supply chain. ZKPs allow for the verification of information without revealing the actual data, providing an additional layer of privacy and security. Companies such as IBM have already implemented blockchain in food supply chain with successful results.

The proposed integration of blockchain technology and ZKPs in the healthcare supply chain has the potential to improve efficiency, transparency, and privacy. Further research is needed to fully evaluate the effectiveness and scalability of this approach in the healthcare industry.

Zero Knowledge Proof (ZKP): is a cryptographic concept that enables a party to demonstrate the truth of a given statement to another party without disclosing any additional information. One widely used implementation of this concept is the Zero-Knowledge Succinct Non-Interactive Argument of Knowledge (zk-SNARK), which is a proof architecture that enable a party to prove that they possess a certain piece of knowledge, such as a secret key, without sharing that knowledge or communicating with either the prover or the verifier. In Ethereum, zk-SNARKs can be implemented by incorporating pre-compiled contracts into the Ethereum blockchain as the building blocks for the verification algorithm. The process of generating the proving key and verification key can be done off-chain. The proving key can then be used to produce a proof off-chain by any prover. The general verification method can then be executed inside of a smart contract, with the input parameters being the proof, the verification key, and the public input. The results of the verification algorithm can subsequently be used to initiate other on-chain processes. This approach enables the integration of ZKPs into the Ethereum blockchain, providing an additional layer of privacy and security for sensitive and confidential data. However, further research is needed to fully evaluate the scalability and effectiveness of this approach in the context of the healthcare industry and supply chain management.

Contributions of the Proposed Work

- Implementation of Blockchain using Zero Knowledge in Ethereum Network.
- Ensuring and protecting the privacy of the business sensitive data without revealing the entire data set.

- Comparing to existing models, our proposed model will consume less time and computation cost.

The paper is organized as follows. Section 2 illustrates the related works in the field of supply chain system related to Blockchain and Zero Knowledge. Preliminaries of the mentioned in Sect. 3. The architecture of the proposed model along with working model is explained in Sect. 4. The system analysis is suggested in Sect. 5. Section 6 discusses the results of paper. Finally, the conclusion of our paper is illustrated in Sect. 7.

2 Related Works

The Zero-Knowledge Succinct Non-Interactive Argument of Knowledge (zk-SNARK) is a type of proof system used in cryptography to demonstrate the existence of specific information without revealing the details. In recent days many researchers works in zk-SNARK. Among them, the first for SNARK is ZeroCash [2]. The authors in [3–7] explained the benefits of using zero knowledge in Blockchain by using Hyperledger in the supplychain management. Out of these, the most efficient and near practical implementations are those built on quadratic arithmetic program. As far as we are aware, the only zkSNARK technique allows data authenticity is ADSNARK [7]. Here, we are using RBAC access control mechanism smart contracts and reducing the time and increasing the computation speed comparing to ADSNARK.

As a basic technology to implement track-and-trace of items across the supply chain in a variety of industries, including food, pharmaceuticals, mining, etc., blockchain has been gaining industry traction over the past decade. [8–12]. The IBM Food Trust [9] platform, created in partnership with Walmart, has been put into use to track food goods from farms to stores, alongside COVID-19 [13]'s continued growth in popularity. The Mediledger solution [13] implemented a zero-knowledge proof based solution in the pharmaceutical supply chain that only gives evidence of transaction while safeguarding the actual transaction data being communicated.

Based on the ring signature method, Monero [14] is a decentralised cryptocurrency that protects user anonymity. All transactions, including transaction amounts, senders, and recipients, can have their transactional privacy maintained. However, it has a big transaction size, and experts have questioned its level of privacy [15]. Therefore, it has been suggested that Bulletproofs [16] generate concise zero knowledge proofs for Monero. It was recently suggested to use ZoKrates [17] to give smart contracts zero knowledge proof. It offers a tool for creating smart contracts and acquiring zero knowledge proofs. The proof is sent to the smart contract for universal verification. However, ZoKrates does not ensure the validity of data for smart contracts.

ZebraLancer [18] is comparable to our work in that it similarly uses zk-SNARK to protect workers' anonymity in a crowd sourcing system built on blockchain technology. ZebraLancer uses the computationally expensive zk-SNARK algorithm to verify complicated digital signatures. With the use of unique arithmetic circuits, we provide a solution that avoids this issues. Recently, the authors in [12] presented an unlinkable supply chain tracing method that protects privacy. They suggest a decentralised tracing method called DECOUPLES that preserves anonymity by utilising blockchain and cryptographic basics like ring signatures and Schnorr signatures. We are eliminating digital signatures and replacing with RBAC (Fig. 1).

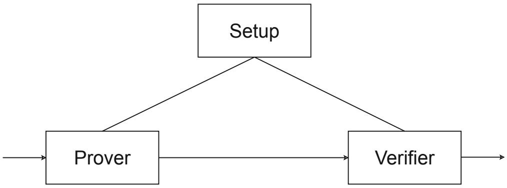


Fig. 1. Arithmetic Circuit

3 Preliminaries

Arithmetic Circuit: This design is made up of wires, multiplication gates, and addition gates and illustrates a function or collection of polynomials as well as their intermediate calculations. This diagram adequately depicts both the computation technique and the function that it represents itself. Every operation in this graph must be right for a computation to be accurate. As we shall see in the subsequent section, we can utilise this structure to construct a proof of the function or polynomial's correct execution. Although the arithmetic circuit associated with a function is not unique, an accurate representation suffices for our needs.

ZK-SNARK of Data Authenticity: Zero-Knowledge Succinct Non-Interactive Argument of Knowledge (zk-SNARK) is a proof architecture that enables the verification of data authenticity without revealing the actual data. It consists of five main algorithms that satisfy the properties of authentication, correctness, zero-knowledge, succinctness, publicly verifiable, non-interactive, and knowledge soundness. These algorithms are as follows:

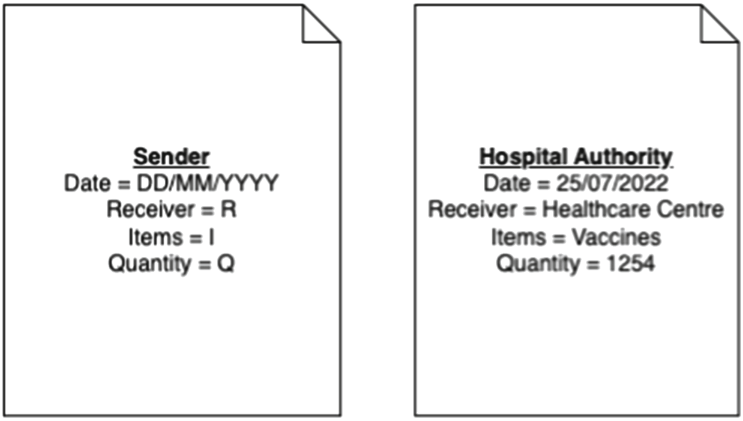
The 5 algorithms are defined as follows:

1. Setup(1^λ) :The setup algorithm generates the parameters Pm necessary for the proof system.
2. KeyGen(Pm,C): Using the program C and the parameters Pm, the key generator algorithm generates the proving key pk and the verification key vk.
3. DataAuth(sk_a,$\vec{x}$): Using a private key KPa, a signature σ, and a vector $\vec{x}$, the data authentication algorithm generates a proof of authenticity for the data.

4. Prove(pk,$\vec{x}$,$\vec{c}$,$\vec{a}$): Using the proving key pk, a public input $\vec{x}$, and auxiliary inputs $\vec{c}$ and $\vec{a}$, the prover algorithm generates a proof π and a computation result R.
5. Verify(vk,pk,π,$\vec{c}$,$\vec{a}$,R,h,σ): Using the verification key vk, the proving key pk, the proof π, the public inputs $\vec{c}$ and $\vec{a}$, the computation result R, a hash value h and the signature σ, the verifier algorithm verifies the proof and returns 1 if the proof is valid or 0 if it is invalid.

In terms of security requirements, the zero-knowledge succinct non-interactive argument of knowledge (zk-SNARK) scheme has several properties that ensure the protection of sensitive and confidential data. These properties include (Fig. 2):

1. **Completeness**: The prover can generate a correct proof if they possess the necessary witness m, and the verifier will always accept the correct proof.
2. **Zero-knowledge**: The prover can prove that they possess a secret m without revealing any information about m to the verifier or any other parties.
3. **Soundness**: Without the proper witness m, it is computationally infeasible for a cheating prover to generate a correct proof. This ensures that the proof system is resistant to malicious actors attempting to cheat the system.
   Together, these properties ensure that the zk-SNARK scheme can be used to verify the authenticity of data without compromising the privacy and security of the data or the parties involved.



Sender
Date = DD/MM/YYYY
Receiver = R
Items = I
Quantity = Q

Hospital Authority
Date = 25/07/2022
Receiver = Healthcare Centre
Items = Vaccines
Quantity = 1254

Fig. 2. Document Format

4 Proposed Work and Working Model

We developed a framework for adding zero-knowledge proofs into supply chain management using blockchain technology in this post. Multiple participants, including National Health Centres (NHC), Hospital Authorities (HA), Primary Healthcare Centres (PHC), Drug Manufacturing Companies (DMC), and Medical Stores (MS), participate in the supply chain model and share information via documents. To provide privacy, authentication, and efficiency in this approach, we suggest using a decentralised application (DApp) with four major actors: the user (U), the authenticator (A), the validators (V), and the Decentralised App (DApp) itself.

Specific tasks in our suggested supply chain model need approval from authorised people. For instance, the authenticator (A) is in charge of producing and signing authentic data for DApp users. Appropriate access restrictions must be implemented in order to guarantee that only authorised people are allocated to this position. In the same way, only authorised validators should be given access to carry out the work of validating transactions submitted to the blockchain system by validators (V).

The DApp has integrated access controls based on user roles to guarantee access control and prevent unauthorised access to sensitive data. This would ensure that users could only access information and services for which they had permission. A user from the National Health Centre (NHC) should be able to access information related to the whole supply chain, but a user from the medical store (MS) should only be able to access information relevant to their store's inventory (Fig. 3).

RBAC systems may be enforced via smart contracts on the blockchain, defining the roles and permissions of each user. With only authorised workers having access to sensitive data, this makes it simple to adopt and enforce RBAC. The supply chain model acquires an extra layer of security by implementing RBAC rules using smart contracts, making sure that only authorised users may access sensitive data.

- **User (U):** The DApp is used by users to access supply chain data and services. They want to guarantee that their data remains confidential when using the DApp.
- **Authenticator (A):** The authenticator is a trustworthy, unbiased data source that generates authentic data and signs it for DApp users using its private key, KP_a. The authenticator is aware of the data's creation time and the users linked with it, but it will never reveal this information to anybody. Anyone with the corresponding public key PKa can validate the signed data.
- **Validators (V):**The blockchain maintainers, also known as validators, are responsible for validating transactions submitted to the blockchain system. A consensus algorithm is used to generate a fresh block of approved transactions. Similarly, smart contracts may be executed on the blockchain.
- **Decentralized App (Dapp):** A DApp is a smart contract that delivers a service on the blockchain. This enables the use of zero-knowledge proofs in managing supply chains while protecting the confidentiality and safety of each individual involved.

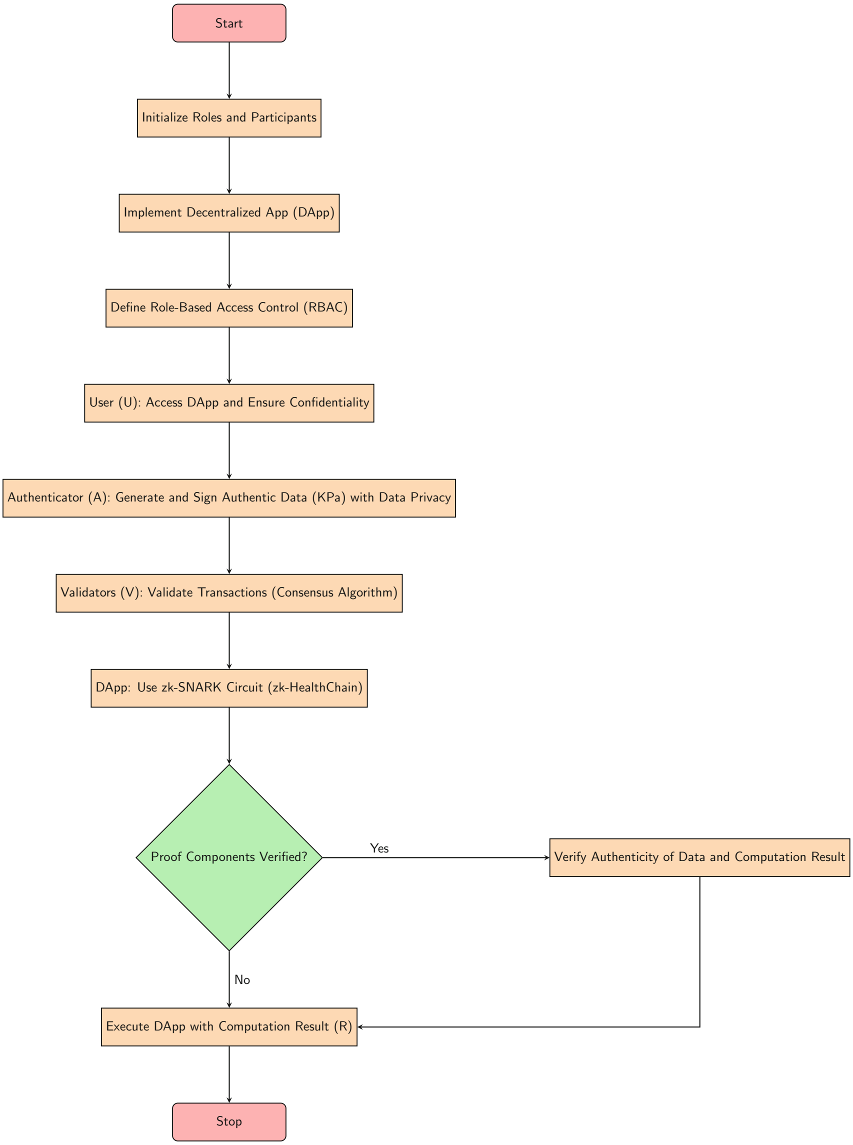

Start
Initialize Roles and Participants
Implement Decentralized App (DApp)
Define Role-Based Access Control (RBAC)
User (U): Access DApp and Ensure Confidentiality
Authenticator (A): Generate and Sign Authentic Data (KPa) with Data Privacy
Validators (V): Validate Transactions (Consensus Algorithm)
DApp: Use zk-SNARK Circuit (zk-HealthChain)
Proof Components Verified?
Yes
Verify Authenticity of Data and Computation Result
No
Execute DApp with Computation Result (R)
Stop

Fig. 3. Flowchart of System Design

4.1 zkHealthChain Model

The proposed model utilizes three vectors as inputs: the DApp user's private data vector $\vec{x} = (x_1, x_2,..., x_n, \text{r})$, the public parameter vector $\vec{c} = (c_1, c_2,..., c_h)$ used for DApp computation, and the public metadata vector $\vec{a} = (\text{ID}, \text{T})$, where ID, T, and r represent the DApp user's identification, time information, and a random number (Fig. 5).

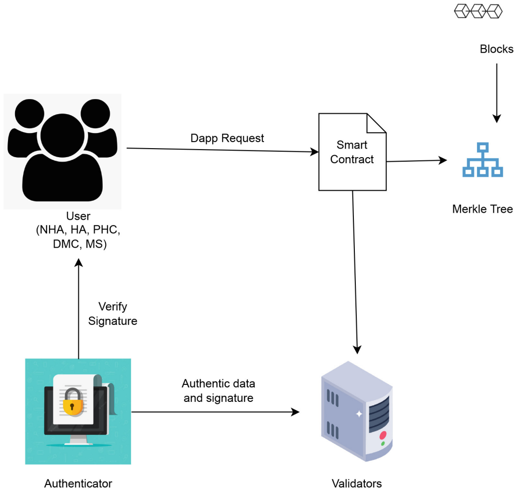


Fig. 4. System Design

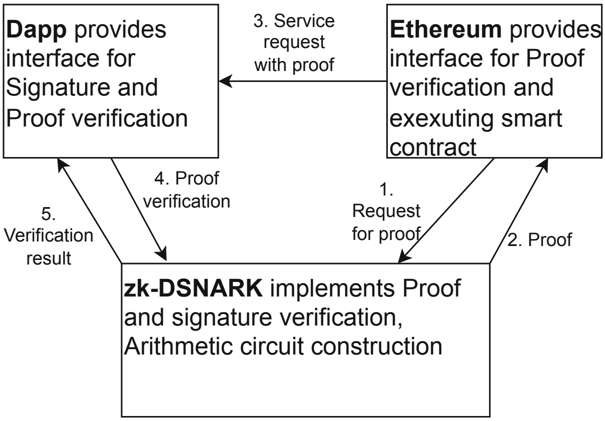

Dapp provides interface for Signature and Proof verification
3. Service request with proof
Ethereum provides interface for Proof verification and exexuting smart contract
4. Proof verification
1. Request for proof
5. Verification result
2. Proof
zk-DSNARK implements Proof and signature verification, Arithmetic circuit construction

Fig. 5. zk-HealthChain Implementation

To keep the user's input private, a random number r is added to the private data vector. The zk-SNARK circuit, zk-HealthChain, is then used to construct a zk-SNARK proof that includes the proof π, vectors $\vec{c}$ and $\vec{a}$, computation result R, hash value h, and a digital signature over h. Following that, the DApp user transmits these components to the DApp for verification. The DApp can determine that the calculation result R is derived from the user's personal data and that the hash value h is generated by mixing $\vec{x}$ and $\vec{m}$. Furthermore, the DApp confirms the authenticity of $\vec{x}$ by comparing the signature's validity (σ) to h. The zk-HealthChain circuit ensures that the same x is used to generate both R and h, which is a remarkable aspect of this model. Furthermore, if the authenticator has signed h, the calculation result R is validated to be based on authentic data.

Setup: The setup step utilizes the function Setup(1^λ) to obtain public parameters Pm.

KeyGen: The key generation step involves the construction of a circuit C based on the computation task required by the DApp. Using a trusted generator and the public parameters pp and circuit C as inputs, the zk-DSNARK scheme is run to generate the proving key pk and verification key vk for proof creation and verification.

Authentication: The authentication step involves the use of the zk-DSNARK.DataAuth standard, which confirms that $\vec{x}$ is authentic and linked to the ID used to identify the DApp user.

Dapp Service Request: The DApp service request step involves the use of the function zk-DSNARK.Prove(pk, $\vec{x}$, $\vec{c}$, $\vec{a}$) to generate the proof π, computation result R, and hash value h. These elements, along with a digital signature σ, are sent to the DApp as a service request in the form of a transaction to the blockchain address of the DApp.

Dapp Service Response: In the DApp service response step, the validators receive the service request and launch the corresponding DApp smart contract function, which separately runs the zk-DSNARK. Verify(vk, KP, π, $\vec{c}$, $\vec{a}$, R, h, σ) function. If the output of the verification function is zero, the transaction is discarded; otherwise, the DApp is run with the computation result set to R. The execution of the DApp is dependent on validator agreement and can only be accepted by the DApp if a majority of validators agree.

5 System Analysis

5.1 Output Privacy

The current implementation of our proposed zk-HealthChain system does not provide appropriate privacy for output data because it is publicly available on the blockchain network. While this information may not directly jeopardise individual privacy, it is nonetheless regarded undesirable. To address this worry, we propose concealing the output data from public view using a comparable zero-knowledge succinct non-interactive argument of knowledge (zk-SNARK) proof scheme. This may be accomplished by modifying the Prove algorithm to provide a proof that corresponds to the circuit shown in Fig. 4. Furthermore, to maintain payment transaction anonymity, we advocate using a zk-SNARK proof system such as Zerocash for payment agreements between the data user (DU) and the decentralised application (DApp) (Fig. 6).

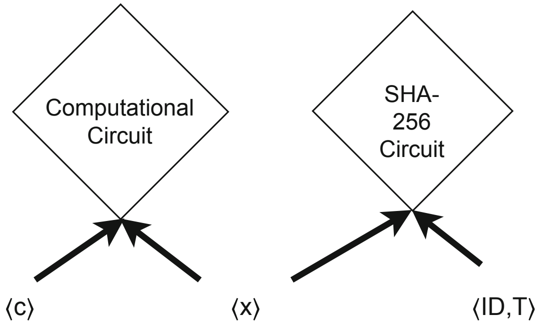


Fig. 6. System Design

5.2 Identity Privacy

The identification (ID) and time (T) of the data user (DU) are disclosed in a public blockchain, which might threaten privacy. To remedy this, as shown in Fig. 4, both SHA256 circuits can receive DU's identifier as a private input. The first hash circuit produces h, which corresponds to a prior zk-SNARK proof for document transactions. A data authenticator needs to authenticate the output of the second hash circuit, h, for a document to be regarded legitimate.

The compensation amount R is generated by the claim computation circuit and paid to DU via the payment circuit. We can retain anonymity while preserving the integrity and legitimacy of the blockchain system by implementing privacy safeguards like these.

Adopting this technique improves the privacy of blockchain-based systems, especially in sensitive industries such as healthcare, where data security is critical. As a result, blockchain technology will become more generally recognised and trusted across a wide range of industries, benefiting both businesses and consumers. Future study should look on ways to improve privacy and security in blockchain-based systems in order to keep this technology growing and being adopted.

5.3 Security Analysis

The proposed zk-HealthChain system makes use of a public blockchain network to maintain the validity of documents transferred among many participants in the healthcare supply chain in a safe and private manner. Private inputs, such as the identify of the document uploader (DU), are processed using SHA256 hash circuits using the zk-SNARK protocol. The result is a commitment value, h, which corresponds to a prior zk-SNARK proof for the transaction. The legitimacy of the document is certified by the data authenticator's (DA) digital signature on the commitment value, h. Furthermore, the system includes a compensation circuit that allows for safe and confidential money transactions between the DU and the decentralised application (DApp).

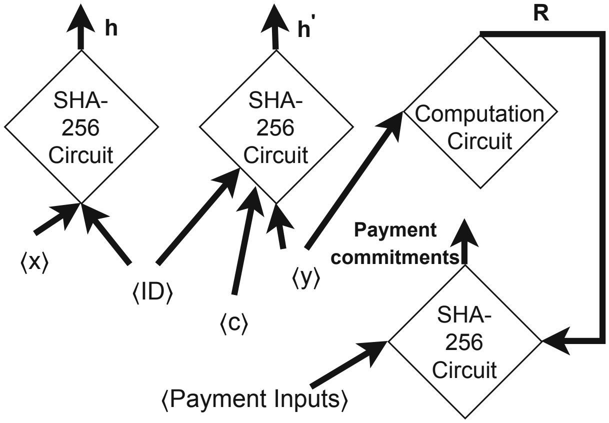


Fig. 7. System Design

1. To ensure RBAC, smart contracts are used to specify the roles and permissions of each user: Smart contract notation: $SC(role, permission)$

   For example, a validator may have the following smart contract: SC(validator, validate_transactions)
2. To generate a zk-SNARK proof for a transaction with RBAC, the private inputs, such as the identity of the document uploader (DU), are processed using SHA256 hash circuits and combined with the role of the user: Hash function H: $\{0, 1\}^* \rightarrow \{0, 1\}$n.

   h = H(DU, d, role), where d is the document being uploaded and role is the user's role in the system.
3. The legitimacy of the document is certified by the data authenticator's (DA) digital signature on the commitment value, h, as well as their role in the system: Digital signature scheme (SK, VK, Sign, Verify)

   σ = Sign(SK_DA, h, role_DA)
4. To perform a compensation transaction with RBAC, the smart contract checks the user's role and permission before executing the transaction: C = (P, V, E, T, s)

   if SC(role_DU, compensate) and SC(role_DApp, accept_compensation) then execute transaction

The zk-HealthChain system, designed for effectiveness, security, and privacy safeguarding, employs advanced cryptographic techniques like as zk-SNARKs to assure the validity of documents transferred on the blockchain network. The incorporation of RBAC mechanisms using smart contracts and the combination of user roles with private inputs ensures that only authorized personnel can access sensitive data and perform certain actions within the system. This strategy has the potential to transform the healthcare supply chain by ensuring strong privacy and security while retaining openness and trust among participants.

5.4 Efficiency

Computation Cost: The computation cost of implementing a zk-DSNARK scheme can be evaluated by the number of gates required for the underlying arithmetic circuit. A simple calculation function can be implemented with a relatively low number of gates, whereas a SHA256 circuit has a significantly higher number of gates, roughly 27,280 gates [4]. The prover is responsible for generating the proof, while numerous validators perform the verification. However, due to the succinctness of the zk-DSNARK approach, the proof can be generated in a matter of seconds.

Key Size: In terms of key size, the zk-DSNARK scheme is comparable to the zk-DASNARK scheme, with both requiring similar key sizes. The key is generated only once and is used for both proof generation and verification.

Proof Size: The succinctness of the zk-DSNARK approach also results in a relatively small proof size. The zk-DASNARK proof is only 288 bytes long and includes a digital signature. The zk-DSNARK proof, on the other hand, has a digital signature and is 128 bytes in size.

6 Results

The experiments are conducted on a PC with Intel Core i5 and 16 GB RAM running 64 bit Ubuntu 20.04. We made a Smart contract of Vaccine Supply and added it to the Dapp. We are considering an equation $E = PK_1.KP_1 + PK_2.KP_2 + PK_3.KP_3 + ...PK_i.KP_i$, where PK_i is Public key of Sender and KP_i is private key of DU. The findings on verification key size, proving key size, circuit gates, key generation time, proof generation time, and verification time are then obtained by increasing the number of private inputs from 10 to 100.

Table 1. Generation Time

Generation Time		
Inputs	ADSNARK	zk-HealthChain
100	16.269	12.339
250	16.358	12.286
500	16.335	12.312
750	16.307	12.376
1000	16.276	12.297

As observed in Fig. 7 Table 1, The both SHA256 circuits and resulting increase in the size of the proving key can be directly linked to the reported results. The circuit size increased as the number of inputs did, resulting in a

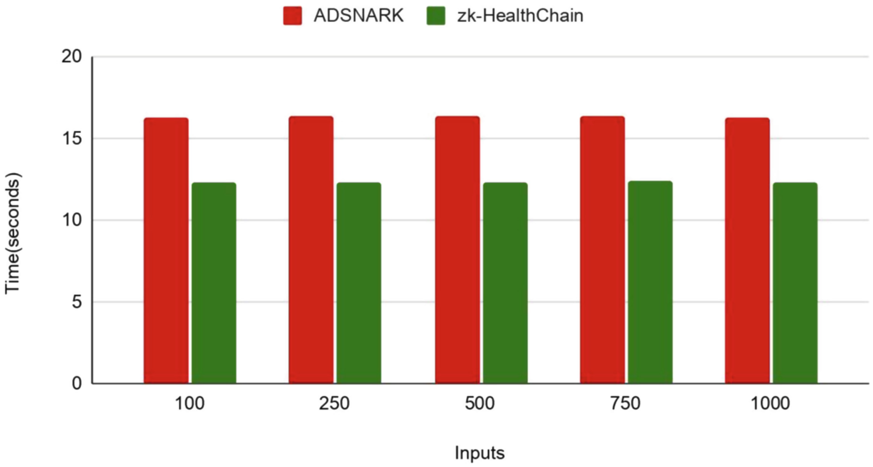


Fig. 8. Generation Time

bigger proving key. The zk-HealthChain system used a smaller 10 MB proving key while the ADSNARK system used a 15 MB proving key when dealing with 1000 inputs. Additionally, when compared to both the ADSNARK and zk-HealthChain models, the zk-HealthChain model showed a 25% decrease in time. The zk-HealthChain model's increased effectiveness and efficiency are demonstrated by this time reduction, which is measured in seconds (Fig. 9).

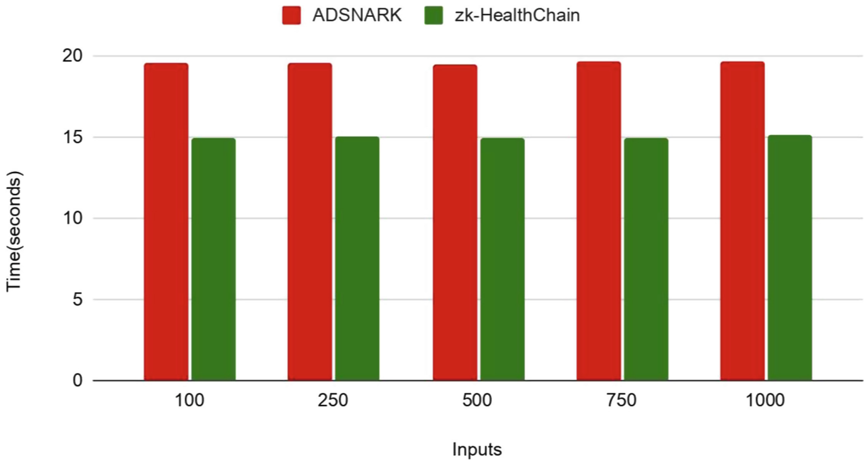


Fig. 9. Proving Time

The results collected from Fig. 8 and Table 2 point to a significant decrease in the circuit's proving time, demonstrating the improved efficiency of the suggested concept. The findings show a notable 20% reduction in proving time, making the suggested model more efficient than ADSNARK. This decrease in proving time not only results in time savings, but also makes it possible to do more computations in a shorter amount of time. Such efficiency advantages have significant effects on a variety of applications, including those needing complicated computations, since they may take advantage of the suggested model's enhanced performance and productivity.

Table 2. Proving Time

Proving Time		
Inputs	ADSNARK	zk-HealthChain
100	19.558	14.978
250	19.597	15.034
500	19.473	14.897
750	19.672	14.904
1000	19.612	15.128

The zk-HealthChain prototype with RBAC-enabled smart contracts includes an additional layer of access control to ensure that only authorized users have access to certain data and functionalities within the system. The RBAC mechanism is implemented using smart contracts based on the Ethereum Virtual Machine (EVM).

In this updated system, the data authenticator and DU are assigned different roles and permissions based on their respective public-private key pairs. The smart contracts define these roles and their associated permissions, and enforce them through access control rules. For example, the data authenticator may have permission to read and write certain medical data, while the DU may have permission to view but not modify the same data.

The evaluation of the RBAC-enabled zk-HealthChain prototype considers the impact of RBAC on the system's performance metrics, including key generation and proof creation times, as well as proof verification times. The size of the proving key and verification key remains the same as the previous prototype, with PK less than 55 MB and VK around 6 KB.

As the number of roles and permissions increases with the RBAC mechanism, the number of gates in the circuit also increases. However, the RBAC mechanism does not significantly affect the time costs for key creation and proof generation, which remain around 8 s and less than 2 s, respectively.

Proof verification times also remain under 16 s, as RBAC does not significantly impact the verification process. However, the time taken to access specific data and functionalities within the system may be affected by the RBAC mechanism, as the access control rules must be evaluated before granting access.

Overall, the zk-HealthChain prototype with RBAC-enabled smart contracts provides an added layer of security and access control to the system without significantly impacting performance metrics.

7 Conclusion

The zk-SNARK protocol, especially the zk-DSNARK version, is used in our proposed solution for data privacy in blockchain-enabled supply chains to solve the issues of safe and private data exchange among multiple supply chain stakeholders. To manage the safe flow of sensitive information, this system use smart contracts on the Ethereum blockchain.

The zk-SNARK protocol, which stands for Zero-Knowledge Succinct Non-Interactive Argument of Knowledge, enables one party to demonstrate to another that they have particular knowledge without exposing the real facts. This is accomplished through the use of a set of cryptographic methods that enable the development of proofs that may be validated by other parties without disclosing the underlying sensitive information.

Incorporating role-based access control (RBAC) into our proposed solution for data privacy in blockchain-enabled supply chains offers an additional layer of security and access control to the system. RBAC allows us to define different roles and their associated permissions based on the user's identity and responsibilities in the supply chain ecosystem. This way, we can ensure that only authorized users can access certain data and functionalities within the system.

By combining the zk-SNARK protocol with RBAC-enabled smart contracts, we can ensure that sensitive data is shared only between authorized parties without disclosing the underlying information. This approach improves system robustness and security while protecting data privacy.

Our suggested solution's implementation displays cheap computing costs and fast transaction speeds, making it ideal for real-world applications. The time expenses for key creation and proof generation rise according to the number of inputs. Proof verification, on the other hand, may be accomplished in less than 40 milliseconds.

Furthermore, the zk-SNARK protocol enables fault detection within the system without revealing important information to other network users. This feature improves system robustness and security while protecting data privacy.

Overall, our proposed solution offers a dependable, effective, and privacy-preserving mechanism for handling sensitive data in blockchain-enabled supply chain systems. By incorporating RBAC access control mechanisms, we can further enhance the security and access control of the system while maintaining its efficiency and data privacy features.

References

1. Sahai, S., Singh, N., Dayama, P.: Enabling privacy and traceability in supply chains using blockchain and zero knowledge proofs. In: IEEE International Conference on Blockchain (Blockchain), 2020, pp. 134–143 (2020). https://doi.org/10.1109/Blockchain50366.2020.00024
2. Ben-Sasson, E., et al.: Zerocash: decentralized anonymous payments from bitcoin. In: Proceedings of IEEE Symposium on S&P'14, pp. 459–474, May 2014
3. Wan, Z., Zhou, Y., Ren, K.: zk-AuthFeed: protecting data feed to smart contracts with authenticated zero knowledge proof. IEEE Trans. Depend. Secure Comput. https://doi.org/10.1109/TDSC.2022.3153084
4. Parno, B., Howell, J., Gentry, C., Raykova, M.: Pinocchio: nearly practical verifiable computation. In: Proceedings of IEEE Symposium on S&P'13, pp. 238–252, May 2013
5. Ben-Sasson, E., Chiesa, A., Tromer, E., Virza, M.: Succinct noninteractive zero knowledge for a von Neumann architecture. In: USENIX Security Symposium, pp. 781–796 (2014)
6. Backes, M., Barbosa, M., Fiore, D., Reischuk, R.M.: Adsnark: nearly practical and privacy-preserving proofs on authenticated data. In: Proceedings of IEEE Symposium on S&P'15, pp. 271–286, May 2015
7. Groth, J.: On the size of pairing-based non-interactive arguments. In: Fischlin, M., Coron, J.-S. (eds.) EUROCRYPT 2016. LNCS, vol. 9666, pp. 305–326. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-49896-5_11
8. Abeyratne, S.A., Monfared, R.P.: Blockchain ready manufacturing supply chain using distributed ledger. Int. J. Res. Eng. Technol. **5**(9), 1–10 (2016)
9. IBM Blockchain. IBM food trust (2020)
10. El Maouchi, M., Ersoy, O., Erkin, Z., et al.: Trade: a transparent, decentralized traceability system for the supply chain. In: Proceedings of 1st ERCIM Blockchain Workshop 2018. European Society for Socially Embedded Technologies (EUSSET) (2018)
11. Kim, H.M., Laskowski, M.: Toward an ontology-driven blockchain design for supply-chain provenance. Intell. Syst. Account. Finance Manag. **25**(1), 18–27 (2018)
12. El Maouchi, M., Ersoy, O., Erkin, Z.: Decouples: a decentralized, unlinkable and privacy-preserving traceability system for the supply chain. In: Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing, pp. 364–373 (2019)
13. Forbes. IBM blockchain is growing in the food industry during COVID-19 (2020)
14. Saberhagen, N.: Cryptonote 2.0 (2013). https://cryptonote.org/whitepaper.pdf
15. Kumar, A., Fischer, C., Tople, S., Saxena, P.: A traceability analysis of Monero's blockchain. In: Foley, S.N., Gollmann, D., Snekkenes, E. (eds.) ESORICS 2017. LNCS, vol. 10493, pp. 153–173. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-66399-9_9
16. Bunz, B., Bootle, J., Boneh, D., Poelstra, A., Wuille, P., Maxwell, G.: Bulletproofs: short proofs for confidential transactions and more. In: Proceedings of IEEE Symposium on S&P'18 (2018)
17. Eberhardt, J., Tai, S.: Zokrates-scalable privacy-preserving off-chain computations (2018)
18. Lu, Y., Tang, Q., Wang, G.: Zebralancer: private and anonymous crowdsourcing system atop open blockchain. In: Proceedings of ICDCS'18, pp. 853–865. IEEE (2018)

Blockchain-Based Secure Noninvasive Glucometer and Automatic Insulin Delivery System for Diabetes Management

Divi Gnanesh(✉), Gouravajjula Lakshmi Sai Bhargavi, and G. Naga Nithin(✉)

SRM University, Amaravati, Andhra Pradesh, India
{gnanesh_divi,lakshmisaibhargavi_g,naganithin_g}@srmap.edu.in

Abstract. Post Pandemic there has been a boost in smart health management. Internet-of-Medical-Things (IoMT) has given an end-to-end control system from the diagnosis of the disease to the cure. Security breaches in this type of hardware security can have fatal effects. The paper discusses Insulin delivery system which includes a security model of glucose measurement device along with an automated insulin pump of IoMT framework. The proposed model is used to monitor and control the glucose levels of a diabetes patient. The blockchain-based security solution is developed for the non-invasive glucometer and insulin pump for safe insulin secretion. It is helpful to mitigate challenges which are present in automatic insulin delivery. With the help of machine learning models, several results can be produced with a futuristic approach along with better understanding of the insulin to be pumped accurately.

Keywords: IoT · Blockchain · Healthcare · Glucometer

1 Introduction

Emerging technologies have always had an impact on the lives of people, one such global innovation is the internet of medical things (IoMT) with a market size of 41.17 billion USD in 2020 at a positive growth rate of 71.45%, according to the study by Fortune Business insights. The study also shows an estimate of its growth from USD 30.79 billion in 2021 to USD 187.60 billion in 2028 at a Compound annual growth rate (CAGR) of 29.45% during the 2021–2028 period. IoMT has become a very cost-efficient and reliable method of data collection, with the ability to produce highly accurate data which is readily available to monitor diseases and tracks and prevent chronic illnesses.

Internet of Medical Things: Emerging technologies have always had an impact on the lives of people, one such global innovation is the internet of medical things (IoMT) with a market size of 41.17 billion USD in 2020 at a positive growth rate of 71.45%, according to the study by Fortune Business insights. The study also

Published by Springer Nature Switzerland AG 2024
D. Puthal et al. (Eds.): IFIPIoT 2023, IFIP AICT 684, pp. 149–159, 2024.
https://doi.org/10.1007/978-3-031-45882-8_11

shows an estimate of its growth from USD 30.79 billion in 2021 to USD 187.60 billion in 2028 at a Compound annual growth rate (CAGR) of 29.45% during the 2021–2028 period. IoMT has become a very cost-efficient and reliable method of data collection, with the ability to produce highly accurate data which is readily available to monitor diseases and tracks and prevent chronic illnesses.

In the scope of IoMT, input elements including communication modules, biosensors, and users collaborate to deliver the finest healthcare service in a quick and secure manner. Self-care and early diagnosis are thought to have the greatest influence on enhancing the healthcare ecosystem with the use of IoMT technologies [2].

Machine Learning (ML): Machine learning (ML) has enhanced the use of these sensors in predicting and diagnosing health ailments. It is a branch of Artificial Intelligence (AL) which focuses on the use of data and algorithms to imitate the way humans learn, gradually improving its prediction accuracy. It helps us to find patterns and insights that would be impossible to find manually. With the increasing use of ML in healthcare, patients and healthtech industries has grabbed the opportunity to overcome the existing challenges and build an improved healthcare system with a unified procedure [a].

Blockchain: Blockchain is a decentralised, unchangeable ledger that makes it simpler to store data and manage digital assets in a business network [1]. It can automate transactions without human interference. Figure 1 illustrates simple block addition to Blockchain ledger. The Blockchain technology is further divided into mainly Public and Private Blockchains. Ethereum is an open- source, decentralised blockchain technology with its own crypto-coin named Ether. Vitalik Buterin firstly introduced Ethereum in a whitepaper published in 2013. It helps to develop applications for all blockchain use cases. The Smart contracts term indicates a decentralised autonomous program that run when certain criteria are satisfied and are recorded on a blockchain. They are often used to automate the execution of an agreement so that both parties may be confident in the outcome

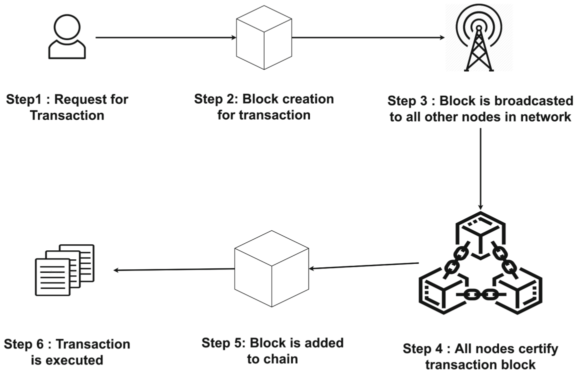

Step1 : Request for Transaction
Step 2: Block creation for transaction
Step 3 : Block is broadcasted to all other nodes in network
Step 4 : All nodes certify transaction block
Step 5: Block is added to chain
Step 6 : Transaction is executed

Fig. 1. Adding a New Block to Blockchain.

without the involvement of a conciliator or the waste of time. They can also automate a workflow by triggering a response when certain circumstances are satisfied.

A block is generated and disseminated throughout the peer-to-peer network, which is made up of computers known as nodes, once a transaction is completed on a blockchain network. A validated transaction might be a bitcoin transaction, a contract deployment, a record alteration, or any other major data activity. When a transaction is approved, it is combined with other blocks to create a new ledger data block

1.1 Contributions of Proposed Work

1. We have introduced a blockchain based decentralized insulin delivery system model to enhance system level transparency and traceability.
2. Developed Smart contracts to automate tracking and used for authentication.
3. Introduced additional sensors like heartbeat sensor to record other daily metabolic activities
4. Implemented an ML model to predict the amount of insulin to be pumped
5. Applying Data Handling techniques to find patterns and predict the possibility of Diabetic occurrences in future

The paper is organized as follows, Sect. 2 illustrates the related works in the field of healthcare. The architecture of the proposed model is explained in Sect. 3. Section 4 represent the system analysis. Finally, we concluded and discussed future work in Sect. 5.

2 Related Works

There are several insulin delivery systems on the market, including as the Mediotronics MiniMed 640G with guardian sensor 3 continuous glucose monitoring (CGM), which requires at least two daily calibrations. Another FDA-approved Tandem Control-IQ system with Dexcom G6 CGM uses an intrusive technique for blood glucose measurement and does not require fingertip calibration [4]. Aminas Vibe technology is more accurate than Dexcom G4 CGM, which corrects blood glucose at the midpoint of the desired range. Similarly, the OmniPod device can provide wireless insulin management without the need for several injections per day. All insulin delivery systems, to the best of my knowledge, either employ intrusive glucose measurement or require repeated calibrations each day. They don't have security features or an autonomous insulin delivery system.

The "intelligent glucometer iGLU 1.0" was offered as a low-cost CGM solution with an accurate noninvasive edge device. It's a portable IoMT device that uses short NIR reflectance and absorption spectroscopy [5]. For accurate glucose prediction, machine learning algorithms were applied. On diabetic, pre-diabetic, and healthy real-world participants, the iGLU 1.0 was calibrated and verified.

The NIR spectroscopy-based gadget employs two short wavelengths in three channels. For optical detection, each channel contains emitters and detectors of a certain wavelength. By using a 16 bit ADC with sampling rates of 128 samples/s, the data are acquired and serially processed. The glucose molecule vibrates at particular wavelengths in accordance with its atomic structure. Short wave NIR areas are found to have greater and sharper absorbance and reflectance. It has been studied how glucose absorbs at its maximal wavelength of 1,314 nm. 23 Utilizing 850, 950, and 1,300 nm, noninvasive blood glucose measurement has been put into practise. 15 The glucose molecule can be detected at a wavelength of 940 nm.

Then, using dual-NIR spectroscopy, iGLU 2.0 was created for exact serum glucose determination. It enables accurate blood glucose determination using a non-invasive method. To obtain precise serum glucose estimation, polynomial regression models and deep neural network 3 (DNN) were proposed [6]. With all types of diabetic patients, the iGLU 2.0 was able to estimate serum glucose from 80 mg/dl to 420 mg/dl.

3 Proposed Work and Working Model

In this article, we have presented a novel architecture model to deal with a decentralized Secure Noninvasive Glucometer and Automatic Insulin Delivery System in IoMT and Blockchain. A closed loop Insulin Delivery System is used here. Every medical device has been assigned with unique ID in the IoMT network. Blockchain is related to every device ID. They have a wallet attached to them for authentication. All of the device-generated data is extracted and saved in CSV files. Machine learning algorithms are applied to a CSV file to get appropriate results and predictions. The doctor reviews the results and signs in his wallet to validate the device. Then, as advised by the doctor, the device releases insulin. As IPFS is used to store all the records, the data is secure and decentralised. No data manipulation is possible. The hospital must manually upload CSV files to IPFS using its website. The hospital should securely store IPFS hashes.

This system has an integration with the machine learning model, helping in the prediction of the diabetes occurrence outcome based on features which include general feature like body mass index, age, gender, blood pressure, skin thickness along with additional lifestyle parameters - like workout, sleep, average heart beat and special parameters like pregnancies, family history of having diabetes and COVID positive. These additional elements bring in a new perspective of how the lifestyle of an individual will help to maintain the blood glucose level. As for the special parameters, it has been observed by several studies, that during pregnancies there is a high rate of fluctuations of the hormones which disturb the insulin secretions in their bodies, thus creating a pseudo diabetic condition till childbirth, in some cases it even lasts for post pregnancy duration and if left uncontrolled turns out to be a true diabetic condition. The exact same pattern was observed after the excess use of steroids post COVID to control the growth of the coronavirus. These features act as an input to the regression machine learning model which then gives the outcome of the insulin to be injected if the person is diabetic.

3.1 Securing and Authentication of Device

Device must be linked to the wallet and online at all times. It creates a blockchain network for the relevant hospital. Only the Chief Doctor, Hospital Authority, and Research Department will be permitted to sign transactions when designing the device. The wallet addresses are hard-coded into the device, and it is the hospital's responsibility to safeguard the seed phrase and private key. Since it uses the SHA 256 algorithm, Blockchain cannot be compromised.

3.2 Regression Machine Learning Model

The collected data is pipelined into a machine learning model, this is a regression analysis that establishes a linear relationship between the feature variables with the insulin predicted. It can be categorized into simple and multiple linear regression with respect to the use of the number of variables being used. While simple linear regression attempts to model a fitting line between two variables, multiple regression is the extension of ordinary least-squares (OLS) regression that involves more than one explanatory variable.

Simple linear regression:

$Y = a + bX + v$

Multiple linear regression:

$Y = a + b_1X_1 + b_2X_2 + b_3X_3 + ... + b_tX_t + v$

Where:

Y = The dependent variable (insulin to be pumped)

X = The explanatory (independent) variable(s) - the features we are using to predict insulin to be pumped)

a = The y-intercept

b = (beta coefficient) is the slope of the explanatory variable(s)

v = The regression residual or error term

4 System Analysis

Smart contracts are deployed on Polygon chain to reduce carbon footprint. Because Polygon uses Proof of Stake (PoS), transactions happen more quickly. We have estimated the total time for file transfer in IPFS utilising the website, Latency, Throughput, and response rate in order to verify the system's accuracy. We have chosen the following file sizes for the experiment: 10 MB, 100 MB, 250 MB, 500 MB, 750 MB, and 1000 MB. When only one node or three nodes are connected, all files are uploaded to the network. In the cases where just one node is connected and when three nodes are connected, all files are uploaded. Machine learning models are trained on local machine consisting of 8 GB RAM and i7 processor along with the GPU.Ml model utilises python library (pandas, scikit- learn, Seaborn etc). GPU being the more utilised element in the training of model with a bigger dataset.

a) Transparency: The overall data manipulation operations are controlled by smart contracts where human interference is eliminated. Because no one has control over smart contracts, system-level transparency is achieved. All the events in the supply chain are recorded, and they are immutable, so tracking changes are effortless. Traditional systems are more venerable to unauthorized modifications and alterations.

b) Immutability: In general, blockchain ledgers are immutable; once they are added to the chain, they cannot be changed or removed. In a traditional database, data can tamper.

c) Availability: The P2P blockchain-based system guarantees the data available all the time and eliminates the single point of failure. Further, the data is backed in the cloud for faster access in a secure format.

d) Traceability: By using block metadata, we can trace where the change has happened. However, in a traditional database, it is not very easy to find.

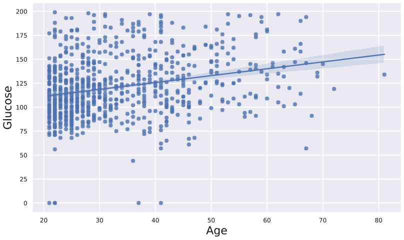
e) Integrity: The data integrity is guaranteed with the help of hash algorithms and blockchain ledgers where the data is stored along with its hash value for any data modification identifications.

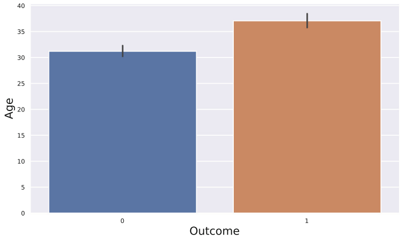
4.1 Total Time for File Transfer

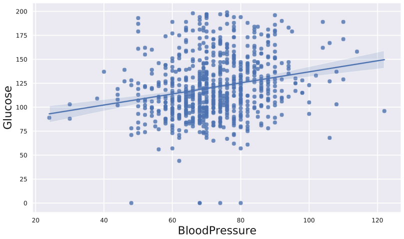
One node's computation duration varied from 9.45 s to 712.45 s. It varied from 12.45 s to 719.455 s for 3 linked nodes. We can observe that as the number of nodes grows, computation time grows as the validator must validate each node (Fig. 3).

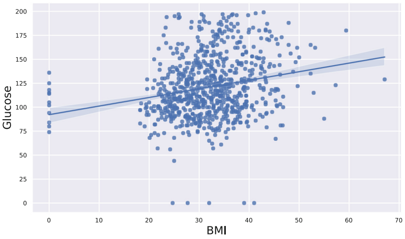
4.2 Latency

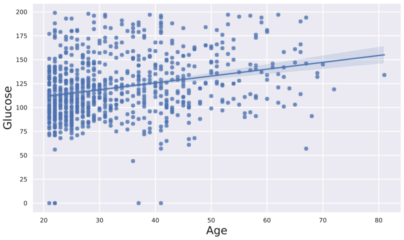
One node's computation duration varied from 2 s to 5 s. It varied from 4 s to 6 s for 3 linked nodes. Transaction latency as the time it takes for a transaction submitted to the blockchain network to be included in a block. This was measured by creating and signing value transfer transactions using the JavaScript SDKs of each network. Transaction latency = The time that a transaction was included in a block - The time that the transaction was submitted to the network (Fig. 2).

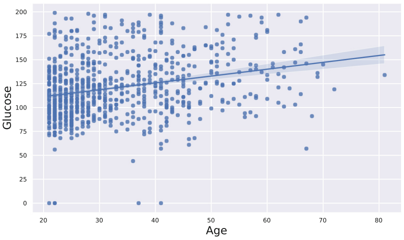

Glucose
0
25
50
75
100
125
150
175
200
Age
20
30
40
50
60
70
80

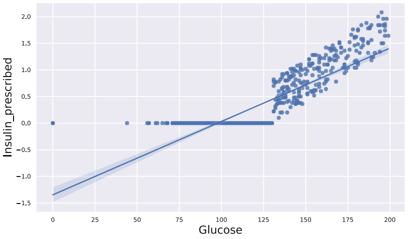

Age
0
5
10
15
20
25
30
35
40
Outcome
0
1

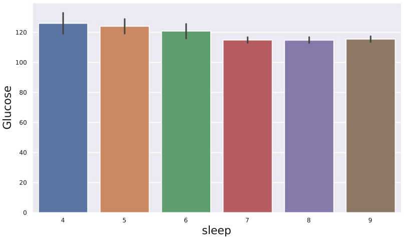

Glucose
0
25
50
75
100
125
150
175
200
BloodPressure
20
40
60
80
100
120

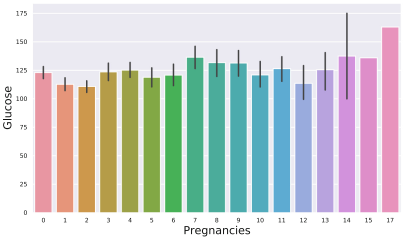

Glucose
0
25
50
75
100
125
150
175
200
BMI
0
10
20
30
40
50
60
70

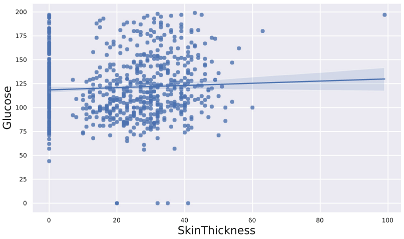

Glucose
0
25
50
75
100
125
150
175
200
Age
20
30
40
50
60
70
80


Glucose
0
25
50
75
100
125
150
175
200
Age
20
30
40
50
60
70
80


Insulin_prescribed
−1.5
−1.0
−0.5
0.0
0.5
1.0
1.5
2.0
Glucose
0
25
50
75
100
125
150
175
200


Glucose
0
20
40
60
80
100
120
sleep
4
5
6
7
8
9


Glucose
0
25
50
75
100
125
150
175
Pregnancies
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
17


Glucose
0
25
50
75
100
125
150
175
200
SkinThickness
0
20
40
60
80
100

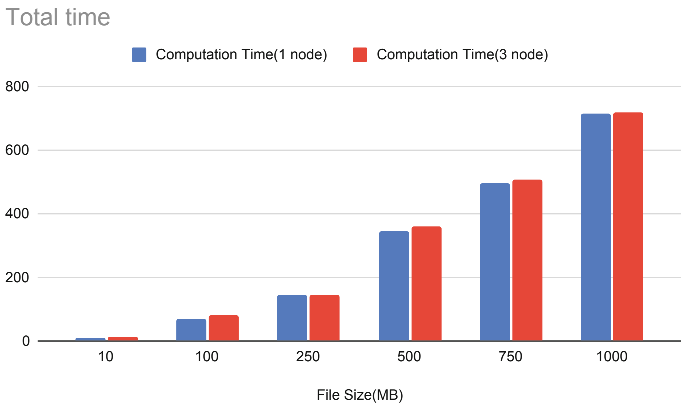


Fig. 2. Total Latency

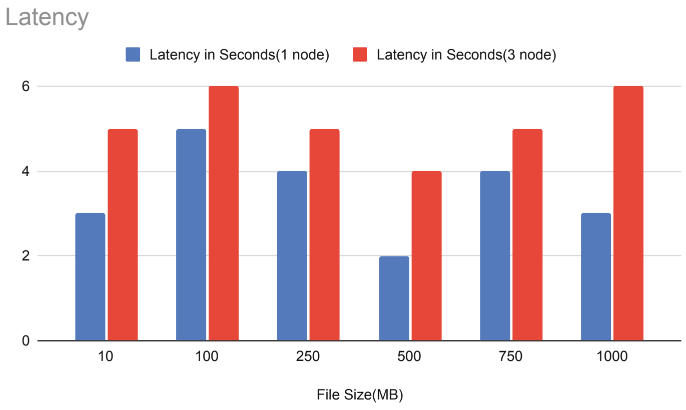


Fig. 3. Total time to transfer files in Blockchain

4.3 Total Throughput Rate

One node's throughput rate varied from 14 to 17. It varied from 16 to 19 for 3 linked nodes. Throughput of the system is the total load that the system handles per unit of time, expressed typically in transactions per second. Throughput increase linearly with increase in nodes (Fig. 4).

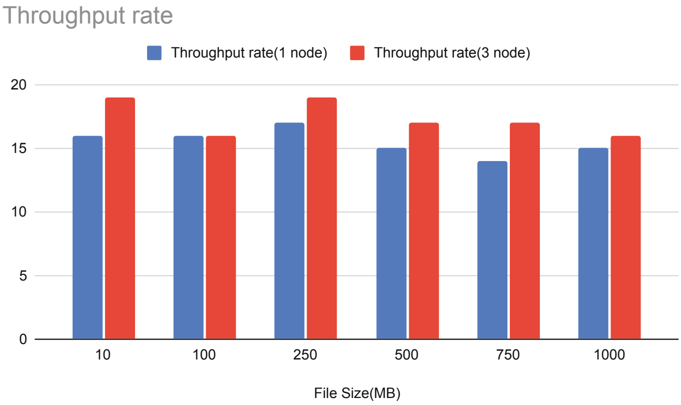


Fig. 4. Total Throughput rate

4.4 Total Response Rate

One node's computation duration varied from 365.453 ms to 476.86 ms. It varied from 409.65 ms to 497.69 ms for 3 linked nodes. Response rate is usually low because we are just calling the data present in blockchain which doesn't need signing of transactions unless specified (Figs. 5 and 6).

4.5 Correlation Heatmap

A correlation plot includes a number of numerical variables, each of which is represented by a column. The relationships between each pair of variables are shown by the rows. Positive values indicate a strong relationship, while negative values indicate a weak relationship. The values in the cells represent the

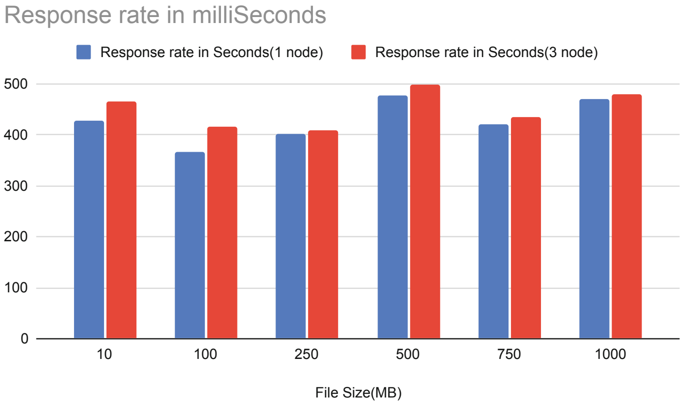


Fig. 5. Total Response rate in milliseconds

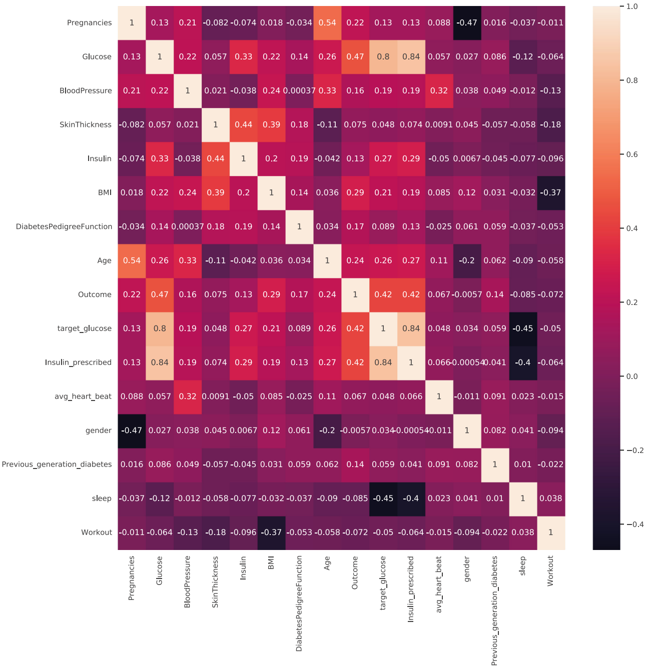


Fig. 6. Heat Map Correlation

strength of the relationship. You can use correlation Heatmaps to identify possible links between variables and to gauge how strong these relationships are. Additionally, outliers can be found and linear and nonlinear correlations can be found using correlation graphs. The cells' color-coding makes it simple to quickly spot any links between the variables. Finding both linear and nonlinear associations between variables is possible with the aid of correlation HeatMaps. This determines the strength in the data set we are utilising.

4.6 Prediction Accuracy

There are error metrics that are commonly used for evaluating and reporting the performance of a regression model. The effectiveness of a linear regression model is assessed using the coefficient of determination, often known as the R2 score. What can be predicted from the input independent variable is the level of variation in the output dependent characteristic and Root Mean Square Error is the residuals standard deviation(prediction errors). Data points' distance from the regression line is gauged by residuals. Residuals are a measure of how far from the regression line data points are. The root-mean-squared error of the model is 0.101 and the r2 score is 0.866.

4.7 Data Analysis

To ascertain whether there is a relation between two variables, regression analysis is performed. To accomplish this, a line that best matches a set of data pairs is constructed. To find the line that "best fits" the data, we shall apply linear regression. We apply regression to find the slope of the best fit line which determines the dependency of variables on each other. Here we considered relation between various independent variables with the glucose as the predicted values have a greater dependency on this feature. We perform various data analysis on the available data set to extract patters like what age group are the individuals more prone be to diabetic. Similar patterns can be generated to analyse and extract the information to provide a better treatment.

5 Conclusion and Future Work

Data generated from the glucometer is channelised into the machine learning model to predict the required insulin units to be given to patients with hyperglycemic i.e. diabetic condition to reduce the blood glucose level inside the body. This data is further transmitted into blockchain which helps in decentralization of data, thus preventing tampering of sensitive content along with maintenance of transparency in the healthcare system, by giving authorized access to only several people. By using this, the power consumption is less compared to PUF hardware.

Using several data analysis techniques on the existing data and adding a few additional parameters into consideration, we are aiming to develop a system to predict several other chronic health conditions like heart attacks, which have diabetes as a pre existing condition. Along with the insulin prediction, we ought to give lifestyle recommendations along with dietary plans to control the calories consumption and burnout to the patients.

References

1. John, J.T., Ramson, S.J.: Energy-aware duty cycle scheduling for efficient data collection in wireless sensor networks. IJARCET Vol. **2**, 1–7 (2013)
2. Özbay, Y., et al.: A fuzzy clustering neural network architecture for classification of ECG arrhythmias. Comput. Biol. Med. **36**, 376–388 (2006)
3. Manickam, P., et al.: Artificial Intelligence (AI) and Internet of Medical Things (IoMT) assisted biomedical systems for intelligent healthcare. Biosensors **12**(8), 562 (2022). https://doi.org/10.45390/bios12080562
4. Berget, C., Lange, S., Messer, L., Forlenza, G.P.: A clinical review of the t: slim X2 insulin pump. Expert Opin. Drug Deliv. **17**(12), 1675–1687 (2020)
5. Jain, P., Maddila, R., Joshi, A.M.: A precise non-invasive blood glucose measurement system using NIR spectroscopy and Huber's regression model. Opt. Quant. Electron. **51**(2), 51 (2019)
6. Joshi, A.M., Jain, P., Mohanty, S.P., Agrawal, N.: iGLU 2.0: a new wearable for accurate non-invasive continuous serum glucose measurement in IoMT framework. IEEE Trans. Cons. Electron. **66**(4), 327–335 (2020)

An Efficient and Secure Mechanism for Ubiquitous Sustainable Computing System

G. Naga Nithin(✉)

SRM University, AP, Amaravati, India
naganithin_g@srmap.edu.in

Abstract. Internet of Things (IoT) devices are frequently utilized to collect information around humans' daily routine, producing a need for them to regularly pair with each other. With the increasing interest in digitizing human's natural environment and evolution of advanced application scenarios, the wireless communication networks have turned into a key player for IoT devices. As IoT devices are resource-constrained and transmit the perceived information regularly to its corresponding participant, it is mandatory for the devices to adopt a lightweight authentication scheme to overcome their limited energy availability and avoid security and privacy issues in ubiquitous sustainable computing system. Researchers have proposed protocols for IoT devices in wireless communication networks, many of which neglect numerous serious security weaknesses such as loss of identity preservation, vulnerability to replay, Man-in-the-Middle, eavesdropping attacks, and loss of key secrecy. Additionally, various security and efficiency threats in the proximity-based device authentication scheme, such as device cloning and identity loss, have a large signaling overhead. Furthermore, we evaluate the performance of the proposed schemes in terms of computation, communication and storage overhead. The results illustrate the implementation advantages and suitability of the proposed schemes for low-powered devices compared to existing protocols.

Keywords: Wireless network · IoT · privacy-preservation · security analysis · sustainable development · energy-efficient

1 Introduction

A natural communication between them that takes place when they are close to each other but fails to maintain a trusted channel or environment has evolved as a result of the widespread usage of wireless devices and equipment. At compatible point of sale terminals, customers may utilise the electronic wallets on their mobile device to make contact less payments. They will couple their mobile phones or devices with nearby resources like Bluetooth, WiFi, or cellular networks in order to broadcast and receive encrypted communications. Securing

Published by Springer Nature Switzerland AG 2024
D. Puthal et al. (Eds.): IFIPIoT 2023, IFIP AICT 684, pp. 160–175, 2024.
https://doi.org/10.1007/978-3-031-45882-8_12

these connections is a key requirement for the ubiquitous development of instinctive communication among devices for protection against masquerading or eavesdropping attacks where an adversary may learn or inject messages between two devices without either device realising about the compromised channel [1,2]. Unlike WiFi-direct, WiMax, or WLAN, the D2D communication uses a licensed spectrum, which may improve network realization and offer access subscribers with an assured quality of services. The Third Generation Partnership Project (3GPP) has also standardised D2D communication technology under the name '*Proximity-Based Services*' [3,4]. As per the standard specifications, proximity-based device communication enables information exchange, social network services, and conference services. Also, proximity-based device communication is subject to a variety of security vulnerabilities due to the direct connections formed between physically close devices [5].

According to the current security aspects of the 3GPP standard for the proximity-based services [6]. However, extensive research has found that the protocol still fails to fulfill key security objectives and is vulnerable to IMSI (International Mobile Subscriber Identity) catcher attack (compromise subscribers' privacy because their identities were not preserved at the time of transmission), de-synchronization attacks, and impersonation attacks [7,8].

Most of the protocols adopt the public key operations to preserve the devices' identity. However, it can be observed that these protocols are vulnerable to security weaknesses such as the replay attack, launched initially for earlier cellular networks that compromises the unlinkability [9–11], loss of identity preservation, key leakage, failure of key forward/backward secrecy, and various other security attacks. Subsequently, modifications of the authentication scheme have been discussed by the researchers in the literature [12–16]. Still, these modifications adopt the public key cryptosystem, which might pose an issue for extreme low power IoT devices due to high resource requirements.

1.1 Technical Contributions

In this paper, we propose a secure and lightweight AKA protocol in the wireless communication network. The contributions of the proposed protocol are summarized as follows:

1. The proposed protocol provides mutual authentication between the UE and the network. Also, the protocol maintains the integrity and confidentiality using Message Authentication Code (MAC) during an authentication process over the communication channel.
2. Compared to the existing solutions, our proposed scheme is very efficient because it only realizes the XOR and symmetric key operations.
3. The proposed scheme achieves various security characteristics such as unlinkability, key forward/backward secrecy, and identity-preservation. Also, the protocol avoids all the identified attacks in the literature.

The remaining sections of this article are arranged as follows. Section 2 discusses the existing schemes. Section 3 illustrates the protocol and its security vulnerabilities. Section 5 presents the authentication protocol. The security model, notations, and security analysis are shown in Sect. 6. The performance evaluations of the proposed scheme is presented in Sect. 8. Finally, Sect. 9 concludes this article.

2 Related Work

Due to common attack attempts in the wireless protocols, researchers and practitioners have proposed various protection mechanisms in the literature [17,18]. Arapinis et al. [9] recommended that the distinct message types of the device's response to the serving network (SN) be encrypted by the HN's public key to create indistinguishability. However, Fouque et al. [10] suggested that the Arapinis's scheme fails to address the replay attack and an adversary may breach the unlinkability in the scheme. In [11], Koutsos et al. proved that Fouque's protocol is susceptible to de-synchronization attacks. Presently, two variations of the wireless scheme are suggested by the researchers, neither of which can be exploited using known techniques. The first is the protocol defined in [11], which is made up of two subprotocols: (i) Globally Unique Temporary Identity (GUTI); (ii) Subscriber Permanent Identifier (SUPI). These protocols were created using just the cryptographic primitives accessible in the USIM, which confined them to the one-way crypto-functions and public key cryptosystem. Furthermore, these operations are necessary for the SUPI protocol if no GUTI is transmitted between the HN and user.

Another scheme, also confined to key operations requires a public key infrastructure for each call session [12]. This protocol establishes the key forward secrecy by generating the secure session key. Basin et al. [13] explained a complete formal proof of wireless- protocol with the Tamarin Prover tool [6] and conclude that the protocol fails to mandate some necessary security properties such as (i) the key establishment between SN and UE is abandoned because the SN fails to determine the genuine session key with the UE; (ii) the protocol is susceptible to the traceability attack. Jover et al. [7] investigated the wireless-protocol and discussed some impractical hypothesis that may provide wireless network susceptible to the potential attacks. Similarly, Cremers et al. [19] analyzed the key security issues of the wireless- protocol such as impersonation attack against the legitimate UE.

Furthermore, Braken [14] proposed the symmetric-key based wireless- protocol to obtain unlinkability, confidentiality, and mutual authentication between user and HN. However, Munilla et al. [20] showed that [14] suffers from loss of key forward secrecy, offline brute force attacks lead to breach of master key. Munilla et al. [20] proposed a new protocol that overcomes the security weaknesses of the Braken's protocol. However, this new protocol requires multiple key updates at user and HN for the subsequent communication. Moreover, the protocol incurs large transmission and communication overhead during the session key and mutual authentication establishment. Recently, Liu et al. [15] and Cao et al. [16] proposed a random number-based challenge-response mechanism to avoid replay attack and conforming the session key secrecy. The protocol adopts the public/private key pair of the HN and one-way keyed cryptographic functions to authenticate the request/response of the user and HN. The protocol obtains most of the security characteristics but incurs huge communication and computation overhead. Similarly, Wang et al. [8] proposed the Diffie-Hellman (DH) key-based privacy-preserving protocol that requires extra round trips for key exchange (significantly increase latency) and incompatible with the USIM implementations.

3 Protocol and Its Weaknesses

The protocol establishes mutual authentication and shared secret key to overcome the signaling congestion and protect the public channel between the network and subscribers. In the protocol, the smart gadget/IoT device consists of the cryptographic security and key generation functions, and subscriber-related information. This temporary identity enables avoiding the use of encrypted SUPI and public key operations. At the completion of a successful execution, UE and network have the session key K_{SAK} for the communication between the subscribers and HN.

Now, we will present various attacks performed by the adversary against the protocol.

1. The adversary may obtain the $RAND, AUTN$ message which is transmitted to the corresponding UE from the HN, and replays it to all possible UEs. After obtaining this message, the designated UE verifies the MAC (computed from legitimate K). However, the other UEs will decline to verify the MAC as the received messages have expired after being replayed.
2. If an adversary compromises the SN, the privacy of UE is not preserved. A bogus SN attempts to compile the UE's SUCI authentication messages and occupy the RES transmitted by the UE in a public channel.
3. An adversary generates the transcript of SUCI sent by the respective UE and replays it to HN for the entire sessions of UEs. Then, adversary waits for the response of the UEs for the challenge/request message of the HN.

Additionally, the protocol is vulnerable to post quantum adversary (yields the quantum queries to a quantum algorithm to breach the scheme) as it adopts the Elliptic Curve Cryptosystem (ECC) for obtaining the confidentiality and relies in the ECDLP indistinguishability assumption. A quantum computer may receive the quantum oracles from the adversary and tamper the privacy of the protocol according to the Shor's quantum scheme [21,22].

4 Preliminaries

4.1 System Assumptions

We adopt the following assumptions in wireless communication networks:

1. The secret key K is embedded in the UDM database and USIM during the manufacturing process. The session keys K_{SEAF}, K_{AUSF} are generated by K at the UE and HN.
2. The UDM is treated as a legitimate entity by the AUSF that may not maliciously transmit the messages encrypted by the private key of one UE to others.
3. The communication channel between the UE/IoT devices is public and an adversary may have full control of the network for forming several attacks during the protocol execution.

4.2 Cryptographic Functions

Our protocol adopts different cryptographic functions such as H_1, H_2, H_3, H_4, H_5, H_5^* which are also used in existing AKA protocols. These functions with their inputs and outputs can be described as follows:

1. Function H_1: An irreversible function used to compute the MAC tag and $RES/XRES$ value, as *HMAC-SHA1*.
2. Function H_2: A reversible symmetric encryption function, such as AES-CTR (AES with counter mode). The key/random number and plain-text can compute the cipher-text, and the cipher-text with key/random number is used to obtain the plain-text.
3. Function H_3 and H_4: Irreversible functions such as *HMAC-SHA256*. Input is 512 bits long with key K, with the output of 256 bits.
4. Function H_5 and H_5^*: Irreversible functions such as *HMAC-SHA3*, accepting input of 512 bits with key K and a random number, and computing 256 bits of output.
5. Function Enc/Dec: Used to encrypt/decrypt the communicated messages over the public channel such as *AES-256*. They accept 256 bits of input with $K/TK/K_{SEAF}$ and generate 128 bits of output value.

4.3 Pseudo-Random Function (PRF)

The PRF is $\{0,1\}^k \times \{0,1\}^* \rightarrow \{0,1\}^{k^*}$ which accepts the inputs as secret parameter $K \in \{0,1\}^k$ and data $D \in \{0,1\}^*$. It produces the output $PRF(K, D)$ which is indistinguishable from random string.

5 Proposed Protocols

This chapter shows a authentication and key agreement scheme. IoT devices transmit the authentication response/request messages to HN and SN for obtaining the secure mutual authentication. After obtaining the session key and mutual authentication between UE and HN.

5.1 Authentication Protocol

Initialization:

HN finds the one-time random number r at the time of UE registration and computes the token values X and A. The Table 1 is shown below for the used notations in the scheme with their interpretation. The following steps are required in the setup-phase:

(i) $X = H_6(r2||W_{SN}) \oplus ID \oplus U$

After the initialization, each UE has the tuple $\{A, X, K, ID\}$ and HN has $\{K, ID, W_{HN}\}$.

Table 1. Notation and their interpretation

Notation	Interpretation
$\oplus$	XOR operation
$\|\|$	Concatenation operation
$IMSI$	International Mobile Subscriber Identity
K	Long-term Secret Key between UE and HN
r	One-time random number generated by HN
ID_{SN}	Identity of corresponding serving network
Key_{HN}	Long-term secret key computed by HN
MAC_{UE}/MAC_{HN}	Message authentication code (MAC) computed by UE/HN
$CK/IK/AK$	Cipher key/Integrity key/Anonymity key
$AUTN$	Authentication token
Enc/Dec	AES-based encryption and decryption function (use AES-256)
TK	Temporary key
EV	Encryption value
K_{SEAF}, K_{AUSF}	Key security anchor function, key authentication server function
CF	Concealing function
$RES/XRES$	Response/Expected response value
K_{hu}	Key value transmitted by the HN to UE after mutual authentication

Mutual Authentication and Key Agreement:

Computation of Authentication Request at the UE

(i) Each UE computes the $CK = H_3(R_{UE}||K)$, $IK = H_4(R_{UE}||K)$, and $AK = H_5(R_{UE}||K)$

(ii) LAI is the location area identity of the UE as the SN knows the UE's location and sends it to the HN. Then, append it in the computation of MAC_{UE}. Here, the protocol establishes the integrity of LAI by preventing the network from redirection attack.

(iii) UE sets the time-stamp of UE (T_{UE}) (initially set as 0)
In the protocol, MAC_{UE} is computed to maintain the integrity of the ID_{SN} that averts the network against redirection attack. The adversary $\mathcal{A}$ may launch this attack if it obtains the correct information of the UE. Here, UE consists of the ID_{SN} in MAC_{UE}.

Transmission of Authentication Request to the HN

(i) In response, the SN transmits its random nonce RN_2 to the UE while monitoring the activity of the UE. After sending RN_2 to the UE, the SN waits for a response for a random amount of time (to prevent Denial of Service (DoS) attacks). If the SN doesn't receive an authentication message response in this period, it will re-transmit the request.
The DoS attack exhibits the scenarios where most of the system consists of timeout period of one second. It might be challenging for an adversary to guess the next timeout value, if it is fixed to any arbitrary values. This scheme could be helpful in regulating the attack rate [23]. A bogus UE may execute a DoS attack to the HN/SN. If the bogus UE forges the first and third messages ($TMSI, XRN_3$), the forged message is detected by the HN.

Authentication Confirmation at HN

(i) HN then computes the $MAC^{'}_{UE} = H_1\langle R_{UE}||K||A||C||ID_{SN}\rangle$
In the redirection attack, $\mathcal{A}$ connects to another genuine SN on behalf of the genuine UE and builds a communication channel between the genuine SN and victim UE.
In the proposed protocol, the UE includes ID_{SN} in MAC_{UE} and transmits MAC_{UE} to the HN. If the HN fails to verify the ID_{SN} transmitted by the SN, the authentication request will be declined. Hence, it overcomes the problem of overcharged billing as the integrity of the ID_{SN} is maintained throughout the communication.
(ii) To avoid the replay attack and obtain the freshness of the authentication request, HN computes the $R_t = H^*_5\langle R_{HN} \oplus R_{UE}\rangle$, where R_{HN} is the random nonce selected by HN.
(iii) Now, HN generates the n AVs from the above computed parameters $AV = R_t||AUTN||XRES$. The HN transmits n authentication vectors (AVs) to the SN to authenticate the UE.

Authentication Response to the SN and Update Phase at HN

(i) HN selects/updates the new value of r as r^*
(ii) The temporary key is generated as $TK = H^*_5\langle K||R_{HN}||R_{UE}\rangle$.
(iii) An encryption value is computed as $EV = Enc(X^*||A^*)_{TK}$ and transmitted to the SN with $\{R_t||AUTN||XRES||EV\}$, where Enc is the encryption function.

Authentication Response to the UE:

(i) After receiving the $\{R_t||AUTN||XRES||EV\}$, SN stores the $XRES$ and forwards the $\{R_t||AUTN||EV\}$ to the UE.

Authentication Confirmation and Update Phase at UE

(i) Each UE computes the T_{HN} form the CF and confirms that the $(|T_{HN} - T_{UE}|) \geq \Delta T$. If this iniquity is true, there is a possibility of replayed authentication request from the HN. Otherwise, UE computes the MAC_{HN} and confirms the authentication with the HN.

(ii) Finally, the value A^*, X^* is updated as A, X respectively for the subsequent communication with HN/SN.

(iii) Each UE computes the $CK = H_3\langle R_{UE}||K\rangle$, $IK = H_4\langle R_{UE}||K\rangle$, and $AK = H_5\langle R_{UE}||K\rangle$. It also computes the session keys $K_{AUSF} = KDF\langle CK||IK||AK||CF\rangle$ and $K_{SEAF} = KDF\langle K_{AUSF}||ID_{SN}\rangle$ as computed by the HN.

Authentication Response to the SN

(i) SN verifies the RES with stored RES and confirms its verification. If both these values are equal, UE is authenticated at the SN.

6 Security Analysis

Here, we analyze our proposed authentication protocol that follows the traditional key-indistinguishability games proposed by Bellare-Rogaway [24]. Similar to the Bellare-Rogaway authentication games, they are designed to prove the confidentiality, privacy-preservation, anonymity, and integrity of the proposed protocol. Specifically, the security analysis of the protocol assumes communications with adversaries $\mathcal{A}$ to expose legitimate and fraudulent parties that attempt authenticate at the HN and SN. Also, analysis of the protocol shows the session key secrecy across multiple-phases of authentications between HN and UE as the token values are computed from previous phases.

6.1 Setup and Participants

The authentication games are played between the adversary $\mathcal{A}$ and a challenger $\mathcal{G}$. The $\mathcal{G}$ executes various instances of the protocol Π with establishing only one HN, a set of S_n serving networks $(SN_1, SN_2, ..., SN_n)$, and a set of U_n user equipment $(UE_1, UE_2, ..., UE_n)$. Each UE_i executes one complete session upto P_n phases of Π. We use the notation ${\Pi_i}^n$ for the identifiers of n^{th} phase of Π executed by the UE_i and session parameters computed at these phases. Similarly, SN_j executes one complete session upto P_n of Π and use the notation ${\Pi_j}^n$ for the verification of n^{th} phase of the SN_j. Each session establishes following parameters:

Furthermore, we are realizing the HN impersonation resistance property. It may be possible that $\mathcal{A}$ may impersonate the HN in online/offline communication messages. The UE is transmitting the A, X, C in open air channel. It enables $\mathcal{A}$ to obtain the HN's challenge for the UE and $\mathcal{A}$ may transmit the authenticated response to UE in a separate session. Here, the advantage of winning the $\mathcal{A}$ in operating state is $Adv_{\Pi,\mathcal{A}}^{protocol,S.imp}(q,t) = Pr(Succ_{\Pi,\mathcal{A}}^{protocol}(q,t))$.

The advantage of $\mathcal{A}$ against proximity-based device authentication scheme Π $Adv_{\Pi,\mathcal{A}}^{protocol}(\phi)$ is stated the probability for $Succ_{\Pi,\mathcal{A}}^{protocol}(\phi))$ 1 when there is no identical session of $ssid^*$. Also, the authentication scheme Π is vulnerable to MitM, cloning, DoS attacks, and key leakage if any PPT adversary has no advantage as $Adv_{\Pi,\mathcal{A}}^{protocol}(\phi) < \epsilon$.

6.2 Security Notions

Here, we define the security notions of the protocol and describe its correctness with the existence of the passive adversary.

Notation-1: The protocol Π, $U_n, S_n \in \mathcal{N}$ is strong server impersonation secure if no $\mathcal{A}$ in running in t, executing q oracle queries (corrupting q_s server queries and performing q_{sn} queries per SN per corrupted server for robust secrecy), and executing q key function queries with an advantage of $Adv_{\Pi,\mathcal{A}}^{protocol,S.imp}(q,t) \leq \epsilon$.

Notation-2: For the protocol Π, $U_n, S_n \in \mathcal{N}$, and probabilistic polynomial-time (PPT) adversary $\mathcal{A}$ (strongly-key-indistinguishable), the advantage of $\mathcal{A}$ in winning the key-indistinguishability game is defined as $Adv_{\Pi,\mathcal{A}}^{protocol}(q,t) = |Pr(Succ_{\Pi,\mathcal{A}}^{protocol}(q,t)) - \frac{1}{2}|$, where $Succ_{\Pi,\mathcal{A}}^{protocol}(q,t)$ is the situation for the $\mathcal{A}$ to win the game. We assume that Π is secure for all the $\mathcal{A}$ if $Adv_{\Pi,\mathcal{A}}^{protocol}(q,t) < \epsilon$.

Notation-3: Let Π has the verification efficiency if the execution $\{HN, m^{'}, HN.ps\} \rightarrow (id^{'}, m^{'}, ps^{'})$ is correct in the existence of passive adversary for the session ${\Pi_i}^P.mc_t = m^{'}$, and ${\Pi_i}^P.id = id^{'}$. It can be observed in protocol that the token values X, A are transmitted by UE for the computation of $IMSI$ at the HN. The HN generates the corresponding one-time random number r and $IMSI$. The only objective of this session is to execute the update operation at the HN without terminating the normal execution of the protocol, rather than having an updated state. Therefore, the transmitted UE's values X and A during the execution of protocol allow to obtain each session state.

7 Formal Security Proof

In this section, we analyze the proposed protocols within above mentioned security notations and model that guarantees the confidentiality, integrity, and session key secrecy.

Theorem-1: Any adversary $\mathcal{A}(q,t)$ against strong server impersonation secrecy of protocol Π, the winning advantage is $Adv_{\Pi,\mathcal{A}}^{protocol,S.imp}(q,t)$ using key

Table 2. Comparison of protocols based on security characteristics (SC)

SC	AKA Protocols							
	Wireless protocol [25]	Wang's-AKA [8]	Cao's-AKA [16]	Braeken's-AKA [12]	Braeken's-AKA [14]	Liu's-AKA [15]	Munila's-AKA [20]	Proposed Protocol
SC_0	●	●	●	⊖	●	●	●	●
SC_1	●	●	●	●	●	●	●	●
SC_2	●	●	●	●	⊖	●	●	●
SC_3	●	●	●	⊖	⊖	⊖	●	●
SC_4	⊖	⊖	⊖	⊖	⊖	⊖	⊖	●
SC_5	⊖	⊖	⊖	⊖	⊖	⊖	●	●
SC_6	⊖	●	●	●	⊖	●	●	●
SC_7	●	⊖	⊖	⊖	⊖	⊖	⊖	●
SC_8	⊖	●	●	●	⊖	●	●	●
SC_9	●	●	●	●	⊖	●	⊖	●
SC_{10}	⊖	⊖	⊖	⊖	●	⊖	⊖	●
SC_{11}	●	⊖	⊖	⊖	●	⊖	●	●

SC: Security Characteristics; ●:Yes; ⊖: No; SC_0: Establish mutual authentication; SC_1: Establishment of session key; SC_2: Establishes the KFS/KBS; SC_3: Confidentiality and integrity; SC_4: Identity preservation and unlink-ability; SC_5: Avoid eavesdropping attack; SC_6: Avoid MitM attack; SC_7: Avoid DoS attack; SC_8: Avoid replay attack; SC_9: Avoid redirection attack; SC_{10}: Avoid de-synchronization attack; SC_{11}: Avoid huge communication/computation overhead

functions K_{f_n}. Hence, $Adv_{\Pi,\mathcal{A}}^{protocol,S.imp}(q,t) \leq U_nS_n(\frac{q^2}{2^{MAC}} + 2Adv_{\Pi,\mathcal{A}}^{K_{f_n}}(q,t) + \frac{1}{2^{l-1}})$

Proof: We are using the following *Games* to prove the theorem.

Game G_0: In this game, the $\mathcal{A}$ is active and its objective is to impersonate the HN to the UE's oracles with no online communication. The HN corruptions are allowed here.

Game G_1: The working of this game is similar to the *Game* G_0 with the $Corrupt(P)$ query. The reduction from the *Game* G_0 to *Game* G_1 is $|Succ_{\Pi,\mathcal{A}}^{protocol}(G_0)| \leq |Succ_{\Pi,\mathcal{A}}^{protocol}(G_1)|$.

Game G_2: The working of this game is similar to the *Game* G_1 with the interaction of a single UE. The $\mathcal{G}$ only provides keys, which are related with the registered UE. Hence, the security loss is: $|Succ_{\Pi,\mathcal{A}}^{protocol}(G_1)| \leq U_nS_n(|Succ_{\Pi,\mathcal{A}}^{protocol}(G_2)|)$

Game G_3: Also, this game is indistinguishable to the *Game* G_2 with the condition to only communicate with only one HN. It may gain authentication challenges from legitimate HNs. As we have seen in the strong key-indistinguishability adversarial model, the associated security loss is obtained by key functions K_{f_n}. Now, we apply the *Test* query applicable at the uncorrupted network. It gives a security reduction as $|Succ_{\Pi,\mathcal{A}}^{protocol}(G_2)| - |Succ_{\Pi,\mathcal{A}}^{protocol}(G_3)| \leq Adv_{\Pi,\mathcal{A}}^{K_{f_n}}(q,t)$

Game G_4: We are updating the *Game* G_3 to replace the results with random crypto-functions and they are independent from the input (same output is ordained from same input). Therefore, we obtain $|Succ_{\Pi,\mathcal{A}}^{protocol}(G_3)|$ $-|Succ_{\Pi,\mathcal{A}}^{protocol}(G_4)|\leq Adv_{\Pi,\mathcal{A}}^{K_{f_n}}(q,t)$

8 Performance Evaluations

We evaluate the performance of our proposed protocols by comparing with recently proposed protocols which are discussed in Sect. 2.

8.1 Security Characteristics

Firstly, we compare the security characteristics of our proposed protocol with existing protocols as shown in Table 2. From the Table 2, it can be observed that the protocols [8,12,14–16] are fails to preserve the identity of the UE and suffers from identity catching attack. Because the loss of privacy-preservation, these protocols are vulnerable to eavesdropping and MitM attacks. Also, these protocols are not suitable for resource-constrained IoT devices due to time-consuming public-key operations such as elliptic curve point addition and point multiplication. Braeken [14] introduces a symmetric key based scheme that suits for low-power devices. However, the protocol suffers from various security attacks and fails to overcome the problem of key forward/backward secrecy. Recently, Munila [20] proposed a lightweight authentication scheme to overcome the issues of [14]. However, the protocol [20] is still vulnerable to some of the security weaknesses. Different from these existing AKA protocol, our proposed protocol mandates all the necessary security design characteristics and avoids most of the identified attacks. Also, the protocol incurs less communication, computation, and storage overhead compared to the existing protocols in the literature (Table 3).

It is also observed that the most of the proximity-based device authentication schemes are suffered from huge overheads which are not suitable for the resource-constrained devices. However, our proposed scheme overcomes all the potential attacks launched by adversary and efficiently preserves the identity during devices authentication.

8.2 Communication Overhead

To evaluate the communication overhead, we compute the sizes of the transmitted messages between the communicating participants during the authentication process of the protocols. We refer to the security parameters of the 3GPP and NIST standards as shown in Table 4 to obtain the communication overhead of the protocols [25]. For the communication cost of public key operations, we are considering $ECC\{F_p\}$ over F_p of the subgroup H, order q, where $|q|= 160$ bits and $|p|= 1024$ bits as ECC has identical security as 1024-bit RSA key [34].

Table 3. Comparison of schemes

SC	AKA Protocols								
	Sfire protocol [26]	Zhang's protocol [27]	Shang's protocol [28]	EAP-DDBA protocol [29]	Wallrabenstein's protocol [30]	Braeken's protocol [31]	Gope's protocol [32]	Lee's protocol [33]	Proposed Protocol
SC_0	⊖	●	●	●	●	●	●	●	●
SC_1	●	●	●	●	●	●	●	●	●
SC_2	●	●	⊖	⊖	●	⊖	●	⊖	●
SC_3	●	●	⊖	⊖	●	⊖	⊖	⊖	●
SC_4	●	●	●	●	●	●	●	●	●
SC_5	●	●	●	●	●	●	●	●	●
SC_6	●	●	⊖	⊖	●	⊖	●	⊖	●
SC_7	⊖	⊖	⊖	⊖	⊖	⊖	⊖	⊖	●
SC_8	⊖	⊖	⊖	⊖	●	●	●	●	●
SC_9	⊖	⊖	⊖	⊖	⊖	⊖	●	⊖	●

SC: Security Characteristics; ●:Yes; ⊖: No; SC_0: Establish mutual authentication; SC_1: Establishment of session key; SC_2: Identity preservation and unlink-ability; SC_3: Avoid eavesdropping attack; SC_4: Avoid MitM attack; SC_5: Avoid DoS attack; SC_6: Avoid replay attack; SC_7: Avoid tunneling attack; SC_8: Uncloneability; SC_9: Avoid huge communication/computation overhead

Table 4. Symbol and their sizes (in bits)

Symbol	Size (in bits)
$IMSI/SUPI/ID_{SN}/TID/PID$	128
$r/r^*/R_{UE}/R_{HN}/RAND/R_t/XR_t$	128
$RN_1/RN_2/RN_3/XRN_3$	64
$K/Key_{HN}/CK/IK/AK/TK$	128
$EV/CF/X/A/C/K_{hu}$	128
$K_{AUSF}/K_{SEAF}/KDF$	256
$MAC_{UE}/MAC_{HN}/RES/XRES/Hash$	128
$SQN/XSQN$	48
T_1/T_2 (time-stamp)	64
ECDH key	256
Chebyshev Polynomials	256
Output of the PUF	504
FE randomness	256
Key for the PRF	128
hd (helper data)	1264

The communication overhead of the schemes are computed in Table 5. The wireless AKA [25] and Wang's AKA [8] schemes adopt the randomized public key encryption and one-way functions. Also, the HN transmits the K_{SEAF} in open air and repetitive messages $RAND, AUTN, SUCI$. Similar, to these pro-

Table 5. Communication overhead of authentication protocols: Comparative summary

Protocols	**Overhead between participants**		
	$UE \rightleftharpoons SN$	$SN \rightleftharpoons HN$	$UE \rightleftharpoons HN$
Protocol [25]	1152	1664	-
Wang's AKA protocol [8]	1152	1664	-
Cao' AKA protocol [16]	1536	640	640
Braeken's AKA protocol [12]	896	1024	-
Braeken's AKA protocol [14]	-	-	1152
Liu's AKA protocol [15]	1248	1376	-
Munila's AKA protocol [20]	-	-	1280
Proposed AKA protocol	1344	1280	-

Proximity-based protocols	**Overhead between participants**
	$UE_i \rightleftharpoons UE_j$
Ghose's protocol [26]	2880
Zhang's protocol [27]	2912
Shang' protocol [28]	2144
Sun's protocol [29]	2720
Wallrabenstein's protocol [30]	3240
Braeken's AKA protocol [31]	3072
Gope's AKA protocol [32]	2296
Lee's AKA protocol [33]	2928
Our Proposed protocol	2416

tocols, the Cao's-AKA [16] and Liu's-AKA [15] suffers form huge communication overhead because the UE,HN are using the ECDH key and ECC-based multiplicative operations. The communication overhead of the Braeken's-AKA [14] and Munila's-AKA [14] schemes are less compared to the proposed protocol because these schemes are establishing the communication between UE and HN only. Also, Braeken's-AKA [16] shows very less overhead but the protocol don't establish mutual authentication between SN and UE. Also, the protocol suffers from several security weaknesses and loss of identity preservation. Our protocol consists of seven number of message communications and adopts the AES-based, HMAC, and XOR operations only. Therefore, the proposed protocol is the best suited solution for the low-power IoT devices authentication in numerous applications.

In the Table 5, we are also presenting the communication overhead of existing and proposed proximity-based authentication schemes. To compute the communication overhead of the PUF-based protocols, we are adopting the system implementation design of Aysu et al. [35]. For the implementation, we are using the 128 bit SRAM-PUF, BCH *FE.Gen*, and *FE.Rec* mechanism. From this implementation, we have noted the key length and data sizes (in bits) of various symbols used in these protocols as shown in Table 4.

The protocols [26,27,29] obtain the mutual authentication and secure session key between proximal devices. However, all of these protocols are using the time-consuming modular exponentiation and ECC-based multiplicative operations. In our proposed protocol, the devices are transmitting the helper data output, MAC value, and token values only. Therefore, the overall communication overhead of our protocol is less compared to the existing schemes.

9 Conclusion

To obtain the energy efficient systems for sustainable smart environment using ubiquitous computing and strengthen the implantation of IoT devices in different application environments, the wireless network is well suited communication technology. One of the elementary security issues for this IoT infrastructure is to mutually authenticate the communicating participants (IoT devices) in communication network. The sensed information is transmitted to the devices frequently; hence, a secure and lightweight authentication protocol for the proximal devices is required to propose. To accomplish these objectives and overcome the discussed security issues. The proposed protocols avoid the problem of key leakage, loss of identity, and numerous security attacks. The formal security proof of the proposed protocols is shown by ROM to conform the correctness, verification, confidentiality, integrity, and key secrecy. Additionally, the performance analysis is conducted for the proposed and existing protocols to evaluate the security strength and competitiveness in terms of security characteristics, communication, and storage overhead.

References

1. Shaikh, E., Mohiuddin, I., Manzoor, A.: Internet of things (IoT): security and privacy threats. In: 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS), pp. 1–6. IEEE (2019)

2. Tawalbeh, L., Muheidat, F., Tawalbeh, M., Quwaider, M., et al.: IoT Privacy and security: challenges and solutions. Appl. Sci. **10**(12), 4102 (2020)
3. Zhou, Z., Dong, M., Ota, K., Wang, G., Yang, L.T.: Energy-efficient resource allocation for D2D communications underlaying cloud-RAN-based LTE-A networks. IEEE Internet Things J. **3**(3), 428–438 (2015)
4. 3rd Generation Partnership Project: Technical specification group services and system aspects; proximity-based services (Prose); (Release 15), 3GPP TS23.303 (2018)
5. Shang, Z., Ma, M., Li, X.: A certificateless authentication protocol for D2D group communications in 5G cellular networks. In: 2019 IEEE Global Communications Conference (GLOBECOM), pp. 1–7. IEEE (2019)
6. 3rd Generation Partnership Project: Technical Specification Group Services and System Aspects; Proximity-based Services (ProSe); Security aspects (Release 15), 3GPP TS 33.303 V15.0.0 (2018)
7. Jover, R.P., Marojevic, V.: Security and protocol exploit analysis of the 5G specifications. IEEE Access **7**, 24956–24963 (2019)
8. Wang, Y., Zhang, Z., Xie, Y.: Privacy-preserving and standard-compatible AKA protocol for 5G. In: 30th {USENIX} Security Symposium ({USENIX} Security 2021) (2021)
9. Arapinis, M., et al.: New privacy issues in mobile telephony: fix and verification. In: Proceedings of the 2012 ACM Conference on Computer and Communications Security, pp. 205–216 (2012)
10. Fouque, P.-A., Onete, C., Richard, B.: Achieving better privacy for the 3GPP AKA protocol. Proc. Priv. Enh. Technol. **2016**(4), 255–275 (2016)
11. Koutsos, A.: The 5G-AKA authentication protocol privacy. In: 2019 IEEE European Symposium on Security and Privacy (EuroS&P), pp. 464–479. IEEE (2019)
12. Braeken, A., Liyanage, M., Kumar, P., Murphy, J.: Novel 5G authentication protocol to improve the resistance against active attacks and malicious serving networks. IEEE Access **7**, 64040–64052 (2019)
13. Basin, D., Dreier, J., Hirschi, L., Radomirovic, S., Sasse, R., Stettler, V.: A formal analysis of 5G authentication. In: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, pp. 1383–1396 (2018)
14. Braeken, A.: Symmetric key based 5G AKA authentication protocol satisfying anonymity and unlinkability. Comput. Netw. **181**, 107424 (2020)
15. Liu, F., Peng, J., Zuo, M.: Toward a secure access to 5G network. In: 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), pp. 1121–1128. IEEE (2018)
16. Cao, J., Yan, Z., Ma, R., Zhang, Y., Fu, Y., Li, H.: LSAA: a lightweight and secure access authentication scheme for both UE and mMTC devices in 5G networks. IEEE Internet Things J. **7**(6), 5329–5344 (2020)
17. Cao, J., et al.: A survey on security aspects for 3GPP 5G networks. IEEE Commun. Surv. Tutor. **22**(1), 170–195 (2020)
18. Ziani, A., Medouri, A.: A survey of security and privacy for 5G networks. In: Ben Ahmed, M., Mellouli, S., Braganca, L., Anouar Abdelhakim, B., Bernadetta, K.A. (eds.) Emerging Trends in ICT for Sustainable Development. ASTI, pp. 201–208. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-53440-0_22
19. Cremers, C., Dehnel-Wild, M.: Component-based formal analysis of 5G-AKA: channel assumptions and session confusion, pp. 1–15 (2019)
20. Munilla, J., Burmester, M., Barco, R.: An enhanced symmetric-key based 5G-AKA protocol. Comput. Netw. **198**, 108373 (2021)

21. Shor, P.W.: Algorithms for quantum computation: discrete logarithms and factoring. In: Proceedings 35th Annual Symposium on Foundations of Computer Science, pp. 124–134. IEEE (1994)
22. Grover, L.K.: A fast quantum mechanical algorithm for database search. In: Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing, pp. 212–219 (1996)
23. Yang, G., Gerla, M., Sanadidi, M.: Defense against low-rate TCP-targeted denial-of-service attacks. In: Proceedings of ISCC 2004, Ninth International Symposium on Computers And Communications (IEEE Cat. No. 04TH8769), vol. 1, pp. 345–350. IEEE (2004)
24. Bellare, M., Rogaway, P.: The AuthA protocol for password-based authenticated key exchange. Contributions to IEEE P1363, pp. 1–8 (2000)
25. 3rd Generation Partnership Project: Technical Specification Group Service and System Aspects; Security architecture and procedures for 5G system (Release 16), 3GPP TS 33.501 V16.1.0 (2019)
26. Ghose, N., Lazos, L., Li, M.: SFIRE: secret-free-in-band trust establishment for cots wireless devices. In: IEEE INFOCOM 2018-IEEE Conference on Computer Communications, pp. 1529–1537. IEEE (2018)
27. Zhang, A., Wang, L., Ye, X., Lin, X.: Light-weight and robust security-aware D2D-assist data transmission protocol for mobile-health systems. IEEE Trans. Inf. Forensics Secur. **12**(3), 662–675 (2016)
28. Shang, Z., Ma, M., Li, X.: A secure group-oriented device-to-device authentication protocol for 5G wireless networks. IEEE Trans. Wireless Commun. **19**(11), 7021–7032 (2020)
29. Sun, Y., Cao, J., Ma, M., Zhang, Y., Li, H., Niu, B.: EAP-DDBA: efficient anonymity proximity device discovery and batch authentication mechanism for massive D2D communication devices in 3GPP 5G Hetnet. IEEE Trans. Dependable Secure Comput. **19**(1), 370–387 (2020)
30. Wallrabenstein, J.R.: Practical and secure IoT device authentication using physical unclonable functions. In: 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), pp. 99–106. IEEE (2016)
31. Braeken, A.: PUF based authentication protocol for IoT. Symmetry **10**(8), 352 (2018)
32. Gope, P., Das, A.K., Kumar, N., Cheng, Y.: Lightweight and physically secure anonymous mutual authentication protocol for real-time data access in industrial wireless sensor networks. IEEE Trans. Industr. Inf. **15**(9), 4957–4968 (2019)
33. Lee, T.-F., Chen, W.-Y.: Lightweight fog computing-based authentication protocols using physically unclonable functions for internet of medical things. J. Inf. Secur. Appl. **59**, 102817 (2021)
34. Bafandehkar, M., Yasin, S.M., Mahmod, R., Hanapi, Z.M.: Comparison of ECC and RSA algorithm in resource constrained devices. In: International Conference on IT Convergence and Security (ICITCS), pp. 1–3. IEEE (2013)
35. Aysu, A., Gulcan, E., Moriyama, D., Schaumont, P., Yung, M.: End-to-end design of a PUF-based privacy preserving authentication protocol. In: Güneysu, T., Handschuh, H. (eds.) CHES 2015. LNCS, vol. 9293, pp. 556–576. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-48324-4_28

Networking and Communications Technology for IoT (NCT)

Understanding Security Challenges and Defending Access Control Models for Cloud-Based Internet of Things Network

Pallavi Zambare(✉) and Ying Liu(✉)

Texas Tech University, Lubbock, USA
{pzambare,Y.Liu}@ttu.edu

Abstract. Access control is one of the most important measures for protecting information and system resources because it prevents unauthorized users from gaining access to protected objects and legitimate users from exceeding their access rights. This paper provides an in-depth exploration of the security challenges posed by the confluence of Internet of Things (IoT) networks and cloud-based architectures, with a particular focus on Access Control Models (ACMs). As the integration of IoT devices with cloud services becomes more pervasive, securing access to resources and data has emerged as a critical area of concern. To address this, we delve into the principles of Access Control and their applications within a Cloud-IoT Architecture. The paper dissects popular ACMs, exploring their strengths, limitations, and suitability for securing Cloud-IoT networks. Along with these the comprehensive analysis of the prevalent Cloud Security Challenges are presented, highlighting the vulnerabilities in current ACMs and proposing potential mitigations. In addition, open research challenges are identified, underlining the need for further investigation and development in this area. The goal of this work is to provide a thorough understanding of the issues and threats in this domain and contribute to the advancement of robust, secure, and efficient access control mechanisms for the evolving landscape of Cloud-IoT networks.

Keywords: Internet of Things · Cloud security · Access control models

1 Introduction

The relevance of meeting security and privacy standards is growing as a result of the proliferation of both cybercriminals and cyberattacks as well as the incorporation of emerging paradigms and technologies such as cloud computing and the Internet of Things (IoT). In addition, the implementation of intelligent industry solutions based on digital and other intelligent technologies is planned. Access control, also known as AC, is one of the most important solutions for ensuring users' privacy in a variety of contexts, including the Internet of Things (IoT), cloud computing, social networks, and other areas. Among the many methods that have been utilized to lessen the impact of their actions, these are among the

Published by Springer Nature Switzerland AG 2024
D. Puthal et al. (Eds.): IFIPIoT 2023, IFIP AICT 684, pp. 179–197, 2024.
https://doi.org/10.1007/978-3-031-45882-8_13

most effective. The access control policy is implemented by the use of an access control system, which regulates not only what users are authorized to access but also when they are allowed to access it, how they are allowed to access it, and what they are allowed to do with it once they have access. This is done to ensure that no unauthorized individuals may have access to either the logical or physical assets [2].

Access control is one of the most important technologies in information security. This stops unauthorized users from gaining access to information and the resources of the system by denying them access. Because of this, genuine users will be able to access information and system resources at the appropriate time periods. Since the early 1970s, the concepts and technologies used for access control have been around for close to half a century, during which time they have undergone a profound transformation from the bottom up, moving from simple to complex systems as well as from theory to practice [6].

At first, only approved users were granted access to the mainframe's shared data. As a direct result of this change, both discretionary access control (DAC) and mandatory access control (MAC) emerged. Because of the DAC's decentralized resource management and extensive permission management, it is not a good choice for large-scale networks with stringent security needs. DAC's flexibility, on the other hand, makes it a good choice for smaller networks. Decentralizing resource management with MAC is one possible solution to the problem; nevertheless, this approach is plagued by extremely rigid authority control. MAC has the potential to cause an excessive amount of burden, poor efficiency, and a lack of flexibility in settings where there are many users and resources that are not clearly defined [8].

Traditional ACMs like DAC and MAC are unable to meet the requirements of modern applications due to the fast development and broad use of computer and network technology. As a direct consequence of this, role-based access control (RBAC) schemes came into being. The RBAC [4] model was presented for the first time in 1996, and subsequent versions include RBAC97, ARBAC99, ARBAC02, and NIST RBAC.

An open network environment needs a hierarchical structure for access control and resource management. Task-based access control (TBAC) is a paradigm for building security models and procedures using tasks [5]. A dynamic and real-time security management system that prioritizes task processing time is one option. Later, TBAC and RBAC were combined to provide task-based access control and delegation models based on tasks and roles. Both models are used. In the 1990s, computer security researchers studied workflow technologies. Workflows are business processes that need many steps to reach a goal. Data is transmitted between users based on criteria. Throughout the course of the workflow, the person that is responsible for carrying out the operation will frequently switch, and their rights will also shift. Dynamic authorization sets security criteria that traditional access control systems are unable to achieve because of their inherent design limitations. As a consequence of this, methods for dynamically constructing an access control matrix with workflow and typical user hierarchy

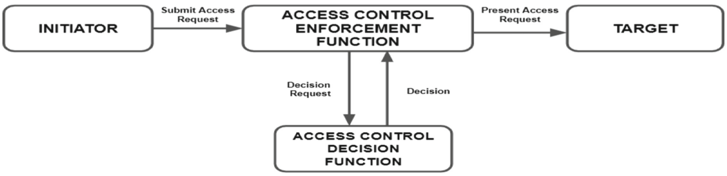


Fig. 1. The process of access control

have been devised. The cloud, the Internet of Things (IoT), and other new computing models can make data sharing easier and deliver more efficient computing services. This has the potential to drastically improve the effectiveness of information exchange as well as the usage of computer and storage resources.

It is imperative that this point be driven home: if these emerging kinds of computing are unable to provide users with an adequate level of protection for their data, then those users will suffer tremendous financial losses. As a direct result of this, cloud access has become a problem that is becoming an increasingly important role in cloud computing. It is conceivable that the data that is kept on the server is not under sufficient control, that it is not effectively safeguarded, or that the computing activity is not being carried out in the right manner. All three of these issues might be causing the problem. As a consequence of this, it is very necessary to develop security policies and architectures in order to protect the availability, integrity, and confidentiality of data that is kept in the cloud.

In the beginning of the paper, we will investigate the evolution of different ACMs and technologies. In Sect. 2, provide an explanation of the fundamental idea behind access control. In Sect. 3, provide an illustration of the architecture of the CloudIOT. The following section, Sect. 4, will discuss the relationships between the various models for the Cloud-Enabled Internet of Things. Address the open research problems in the Internet of Things that are afforded by the cloud in Sect. 5.

2 Basic Principle of Access Control

Access management deals with limiting an accessing subject's access to an accessible object and making data resources available while remaining within the limitations of the law. There are three components that makeup access control: the subject, the object, and the access control policy. The entity that is responsible for initiating both the access request and the access action itself. Because objects are non-active entities that are only capable of accessing other entities, they are the targets of access actions rather than the actors. The access control policy of a subject is the collection of guidelines that determine how the subject can interact with an object. Figure 1 shows the main components and access control authorization method [6]. An access matrix model may represent a system's access control strategy. Lampson abstracted access control before proposing a formal formulation using the subject, object, and access control matrix. The subject accesses the object, and the system uses a reference monitor to regulate access according to the access matrix.

Access rights or access modes are two different ways that authorization can be communicated. Access rights are a broad category that covers many kinds of access. Read, write, execute, and ownership are the four access permissions that are typically granted to files. The meanings of the first three of them are readily apparent. When talking about files ownership refers to who has the authority to make changes to who can access which files. Each cell in the access matrix provides the level of authorization granted to the subject in the row with regard to the item that is located in the column. Each topic has a row, and each column has an item. Access control ensures that only access matrix permitted actions are performed. The reference monitor, which is in charge of mediating any and all object alteration attempts, is the one responsible for achieving this goal. The owner of a file is typically the only person who has the authority to decide which users are permitted access to the file and which users' access privileges are revoked. It's possible that a huge system's access matrix will be quite vast, despite the fact that most of its cells will be vacant. As a direct consequence of this, access matrices are almost never implemented in the form of matrices.

1. **Access Control Lists:**
   A technique that is rather common is to implement the access matrix by using access control lists. An access control list will specify, for each object in the system, whether the subject is permitted to carry out the action of executing the object. The matrix is stored in columns when using this approach. An object's access control list (ACL) is one of the factors that may be used to establish the kinds of access that an object is permitted to accept at the moment. They make accessing and monitoring items very easy. The ACL of every object in the system must be examined to determine how a subject's access is controlled. It is difficult to determine all the subject's access in an ACL-based system.
2. **Capabilities:**
   ACLs might be seen as alternative approaches to the problem. The capacity list is connected to each individual topic. A system that specifies for each item in the system which access the subject is permitted to carry out on it and indicates this for each object in the system. Rows include a matrix of access privileges that may be accessed. When using the capability list method, it is simple to inspect all the access that a subject has. Examining the capability lists of all the subjects in the system is necessary in order to establish which subjects have access to a certain item.
   In general, access control schemes are classified into three major categories as shown in Fig. 2.

   1) Centralized Access Control:
   2) Distributed Access Control:
   3) Hybrid Access control:

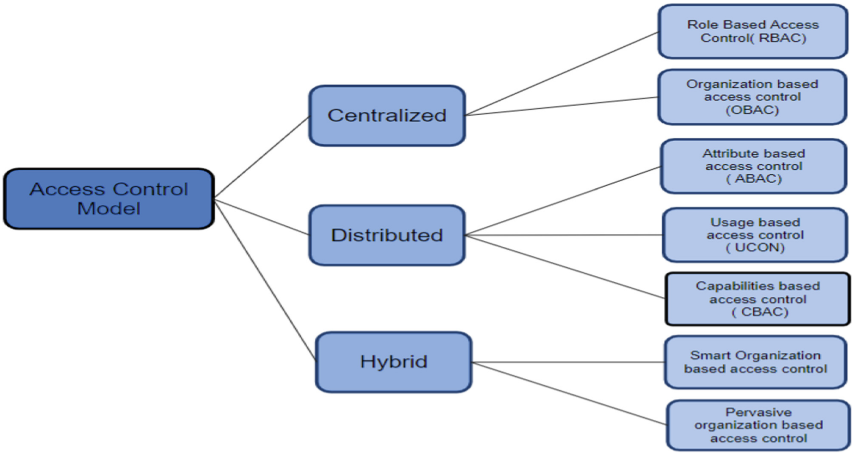

Access Control Model
Centralized
Distributed
Hybrid
Role Based Access Control(RBAC)
Organization based access control (OBAC)
Attribute based access control (ABAC)
Usage based access control (UCON)
Capabilities based access control (CBAC)
Smart Organization based access control
Pervasive organization based access control

Fig. 2. Classification of Access Control Model

3 Cloud-IoT Architecture

Cloud computing and the Internet of Things have experienced rapid growth and development [7]. Their characteristics when integrated together are remarkable. Cloud and IoT complement each other very well, which is why numerous researchers have proposed all possible applications considering the integration of Cloud and IoT. After taking advantage of the availability of support from the cloud in terms of storage and computing capabilities, IoT has benefited greatly.

The IOT provides ease and convenience to human existence anywhere it's implemented. However, due to the diverse structure of the network, its widespread deployment, resource-constrained nodes, and the huge amounts of data that it generates, maintaining its security is a highly critical and difficult task. The architecture of the Internet of Things network is composed of three levels, as depicted in Fig. 3. Even though this is not a typical Internet of Things design, most of the suggested architectures have these different levels. As a result, this the design was chosen to serve as the reference architecture for identifying and organizing the many security issues that arise in the IoT. Figure 3 depicts the IoT architecture that is most frequently recognized. The following are the many levels that makeup IoT:

1. **Sensing Layer:**
   This layer is comprised of equipment like sensors and RFID that can detect any real-world physical event. These devices can detect things like RFID tags, the weather, and the water level in agricultural fields. This layer's essential components include wireless sensor and actuator networks as well as radio frequency identification.
2. **Network Layer:**
   This layer is responsible for safely transmitting the data that has been gathered by the sensor devices located in the perceptual layer to the fog nodes,

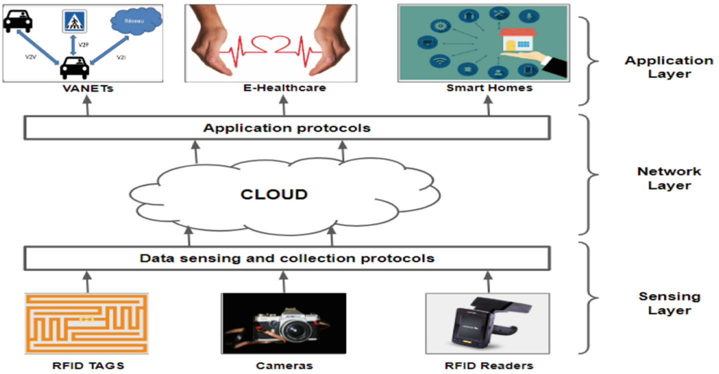


Fig. 3. Cloud-IoT Architecture

the main cloud, or directly to another IoT node. Mobile networks, wireless ad hoc networks, and satellite networks are examples of the many technologies that exist at this layer. These technologies also make use of a variety of trustworthy communication protocols.

3. **Application layer:**
   This layer is responsible for providing services related to the IOT to users in accordance with their requirements. By using the application layer interface, users may have access to a variety of different services. These applications include smart homes, intelligent healthcare systems, intelligent transportation, smart agriculture, and autonomous vehicles, amongst many more [2].

4 Cloud Security Challenges

Even taking into account the significance of IoT and the breadth of its applications, it is not simple to use it in vital application domains where maintaining one's privacy and safety is of the utmost importance. For instance, a successful assault on an intelligent healthcare system might have a negative impact on the lives of many patients, resulting in monetary loss, and even result in the loss of human lives in the case of an intelligent transportation system. The security of the Internet of Things is a difficult subject that requires further study to be able to meet these issues. In the following paragraphs, we will provide a concise overview of these security concerns: [1]

- **Security:**
  The Cloud receives, processes, and stores the data generated by the Internet of Things devices as it is sent there from those devices. Not only is it important to provide the safe transmission of data from the nodes to the Cloud, but it is also necessary to ensure the secure storage and processing of data inside the Cloud. Because there is a dearth of transparency concerning cloud storage, data owners are often ignorant of the geographic placement of their data. Due

to the fact that almost everything in our environment is now connected to data, we regard the protection of data as the most significant obstacle in the world of cloud computing and the Internet of Things.

- **Dependability**
  Cloud services are an essential need for time-sensitive Internet of Things applications and the outcomes have a direct influence on how well the application performs. For example, in the domains of transportation, medical equipment, and applications for the military.
- **Heterogeneity:**
  There are already hundreds of different companies that make the Internet of Things devices; as a result, there is a worry over the smooth interoperability of these devices. As new and enhanced apps are produced in the market to fulfill the expectations of customers, cloud computing has to keep up with the progress of the underlying platforms and protocols of the Internet of Things devices.
- **Intensive Applications:**
  Cloud IoT's strength is serving a variety of heterogeneous applications, but at the same time, it might be considerably difficult to process data gathered from sensors located at a number of geographical locations over long periods of time. Intensive applications require both low latency and high processing power. Consequently, they should be provisioned as quickly as possible.
- **Data Storage:**
  The number of IoT devices will grow to approximately 50 billion by approximately 2025, which means that cloud service providers will face a great challenge in providing timely and safe access to data.
- **User aided IoT devices:**
  Users of certain IoT applications are required to provide information, and in return, they are rewarded with incentives for their efforts. Due to the social aspects involved, where the user contributes from their background, it is a challenging task.
- **Edge Computing:**
  Applications for the Internet of Things that are limited in terms of latency and mobility and are geographically spread must have an immediate response from the cloud. Edge computing, which is analogous to cloud computing but located physically closer to the applications, was developed as a solution to this problem. However, edge computing is challenging to deploy since it needs location awareness.
- **Aggregating Sensor Networks:**
  An IoT sensor network can be used across a wide range of applications and is a disruptive technology. It also raises a number of challenges, such as network uncertainties and energy constraints. As the sensors became mobile, they created new challenges in their own right, and on the other hand mobile phones with their built-in sensors catered to a variety of applications, requiring cloud-based techniques for aggregating sensor data.

5 Access Control Models

Recent research has suggested a great number of innovative strategies for controlling access. Because cloud computing is primarily predicated on the sharing of resources, it necessitates an excessive amount of resource utilization in order to implement stringent preventative measures. Cloud computing for the Internet of Things presents new issues when it comes to managing access technologies and limiting access, because it is a large-scale, dispersed, and virtual information system.

- **Role-Based Access Control (RBAC) based solution:**
  Role-based access control paradigms and frameworks allow users to access resources depending on their responsibilities. In this design, RBAC has four components, each with separate functions. RBAC has core, hierarchical, static, and dynamic components. The core component is the most fundamental and fundamentally important. RBAC's fundamental model is made up of five different components. The first group is comprised of users, roles, and permissions, and the second group is made up of operations performed on objects. The pieces of the core model are grouped in a clear fashion that resembles a many-to-many relationship. A user is given a role, and then the role receives permissions that have been granted to it. The RBAC process is broken up into two main segments. A system administrator is able to delegate a wide range of responsibilities to different components of a computer system using one particular design. The next phase is called the run-time phase, and it is during this phase that the model is responsible for enforcing the system's assignments in accordance with the security policy of the system, which was outlined during the design phase [8].
  It is simple to assign users to roles because of the components of RBAC (role- permissions, user-role relationships, and role-role connections). Figure 4 depicts the connection that exists between RBAC roles and their respective users. RBAC has the potential to make the management of security in large organizations more straightforward and ensure that the information integrity requirements of information systems are met. In the study, the authors take a service-based approach to release IoT, which necessitates that IoT devices expose their functionality in the form of standard services. As a consequence of this, the service is the object of the request, and the authorization of the service must first be validated by access control before the service may carry out the operation. The authors expanded the RBAC model to take into account contextual information by integrating context constraints obtained from the environment of a physical object. This allowed the model to take into account information such as time, position, and the state of the environment. Web services make it possible for different kinds of devices to work together without any problems.
  However, the authors did not explain how the physical object is mapped to one or more web services or, more importantly, how contextual information for the physical object is collected from its surroundings in real-time to be used

in the authorization process. Both of these points are important. The Internet of Things is hampered by a number of restrictions in an environment that is confined by the IoT. These restrictions include reduced flexibility, single-point failures, and large-scale implementations.

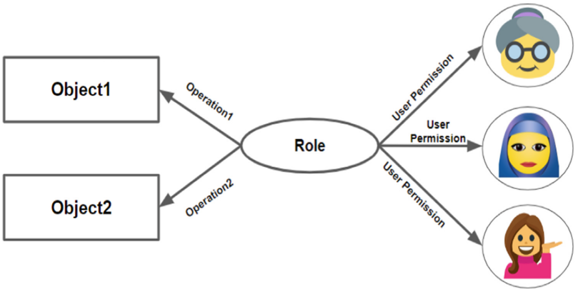


Fig. 4. Role and user relationship of RBAC

- **Organization-Based Access Control (OBAC) based solution:** Based on the theory of an organization, the OBAC system is conceptualized as a group of active entities that are organized into a system. Addition- ally, subject, view, activity, and contexts are integral concepts that can be used to build a security strategy. Subjects can play a role in portraying explicit roles. In this paper, the author proposes a new security policy model that addresses several limitations of previous models [9]. It focuses on an organization centric model called ORBAC. Depending on an organization, a security policy may include other concepts as well:

  1) The way in which this organization uses subject matter is reflected in the concept of Role

  2) The way this organization uses objects is modeled by the concept of View

  3) The concept of activity describes how this organization is acting.

  4) The organization defines contexts relevant to users who act on objects.

  The connection known as "Define" illustrates this point well. Permissions, prohibitions, duties, and recommendations are the building blocks of a company's security policy, and they are specified utilizing the aforementioned ideas. A permission is a fact that has the form Permission (org, r, v, a, c), which indicates that a role r within an organization org is authorized to carry out an action a while in context c. Permission corresponds to a fact that has this form. The interpretations of "Prohibition","Obligation", and "Recommendation" are all quite similar to one another. There are still a lot of issues to be resolved, despite the fact that precise permits, prohibitions, duties, and suggestions have been provided for subjects, objects, and acts.

First, there is the possibility of security policies being in conflict. It is necessary to identify and solve both the cases in which tangible permission can be derived as well as the cases in which it is possible to derive a tangible prohibition for a given subject, an object, and a given action. This is because it is necessary to determine whether a concrete permission can be derived or whether a concrete prohibition can be derived. In order to tackle this issue, you should suggest a logical strategy that is possible and uses automatic prioritization of facts that constitute security policy. Because of space constraints, the challenge of putting into practice a security policy that has been modeled is not tackled in this article. It is very evident that this kind of administration model is required for a full model. In accordance with the ARBAC model, the RBAC security policy administration process can be utilized. In conclusion, the ORBAC model needs to include the specification of security features. The security policy should include mechanisms for determining when it has been breached and what actions are to be taken as a consequence, such as what should be done in the event that duty has not been strictly adhered to [9].
One might speak of an activity as being a collection of acts, and one can speak of a view as being a group of objects. However, the most significant disadvantage of this paradigm is its centralized architecture, which causes a great deal of difficulty. The implementation of IoT devices is made more difficult by problems associated with large-scale implementations as well as the lack of lightweight tools and procedures.

- **Attribute-Based Access Control (ABAC) based solution:**
  ABAC has become a popular ACM in recent times. Using novel concepts, Access Control Management and Access Control Rules are simplified. ABAC evaluates the attributes of several entities and based on this evaluation, decides whether access should be granted or denied. Thus, attributes are major components of any ABAC and play a key role in its construction ABAC grants access to a subject based on attributes presented by the subject. As a matter of fact, the subject and the object are both identified by characteristics associated with attributes [11].

  ABAC model is provided in Fig. 5 Attribute assignment (AA) is the process by which attributes are given to subjects and objects. Policy permission relation (PPR) is the process by which a relationship is established between policies and the permissions they provide. Policy is the term that is used to refer to the collection of rules that regulate access in the system [10]. There are two components of ABAC: the policy model (sometimes called PBAC, or Policy Based AC), and the architecture model to apply the policy. ABAC states that an individual's access can be determined by a number of attributes. Various policy rules stipulate the conditions for granting or denying access. Through the attributes associated with the characteristics, the subject and object are identified. Upon initiating an access request, the system grants the user the appropriate permissions based on his attributes.

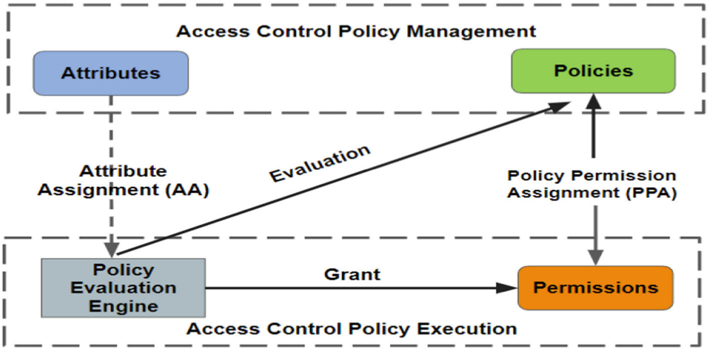

Access Control Policy Management
Attributes
Policies
Attribute Assignment (AA)
Evaluation
Policy Permission Assignment (PPA)
Policy Evaluation Engine
Grant
Permissions
Access Control Policy Execution

Fig. 5. Attribute-Based Access Control (ABAC) model

The security of the (IoT) continues to be plagued by an increasing number of obstacles as the Internet of Things grows increasingly pervasive in people's everyday lives. In order to guarantee the safety of data transmission in WSN and serve as a backup for the IoT perception layer, authentication, and access control mechanisms are required. Traditional cryptographic algorithms are not suitable for use in the open environment of the Internet of Things because they do not fulfill lightweight criteria and do not provide mutual authentication between users and nodes. An ECC-based authentication policy [21] and an attribute-based access control policy were proposed in order to realize the goal of achieving fine-grained access control and mutual authentication between users and nodes. Mutual authentication protects connections between nodes and users. As the authentication procedure itself is straightforward, it is able to circumvent the resource-limiting issue that arises at the IoT perceptual layer. By allowing data access based on user attribute certificates, access control authorities can provide flexible and fine-grained control over who has access to what data [13].

However, despite being more scalable, having finer-grain control, and requiring less communication and storage overhead, this architecture does have a number of drawbacks that need to be considered. Taking into account the restrictive nature of the context in which the IoT system operates, the management and deployment of this model are significant shortcomings. In addition to this, mapping sensor data into attribute values can be problematic as well.

- **Usage Control Based Access Control (UCON) based solution:** According to, usage control (UCON) is considered to be the next generation of ACMs. As compared to traditional access control methods such as RBAC and ABAC, it introduces a number of novelties. The authorization process occurs continuously, before, during, and after the execution of the access. In addition, it supports the mutability of attributes, which means that if an access attribute changes while the access is in progress and the change does not accord with the security policy, access is revoked and usage is canceled. The UCON model offers particularity in the continuity of decision-making and the mutability of attributes.

UCON abstractions map to IoT entities as follows: The device or object of UCON is the device or object in IoT. In IoT, UCON is represented by the device, which includes information about the device's trust value and so on. The Service, which resides in the application layer and queries the wireless sensor network for information on the services it offers, is an integral part of UCON in the Internet of Things. The attribute(O) of a UCON in the IoT is called the attribute(Service), and it stores information about services like the digital sources used for automobile navigation. The policy of UCON in IoT is decided by the wireless sensor network. This policy includes trust value and other elements. In a wireless sensor network, the letter "C" denotes a constraint that is relevant to the current situation, such as the position of the network's nodes geographically. IoT's UCON(B) obligation may be found in its requirements, which can be found in the wireless sensor network's requirements. IoT devices should have duties before or during use control [14].

Device, service, and use control determine IOT Authorization (A). The Device's trust degree and the Service's trust threshold determine access control rules for the Device, the Service, and other information. The calculation is hazy. Despite theoretical trials, this strategy remains unproven.

The collection of subjects, objects, and system characteristics define a logic model's state sequences. Authorization predicates use subject and object characteristics. Usage control activities alter attributes and access usage process status, and obligation actions must be completed before or during use conditions are predicates. Temporal formulae describe the use of control rules using permission, action, and system circumstances. Using scheme rules makes the UCON specification comprehensive and sound. UCON has exact modeling and specification skills due to TLA flexibility and enhanced specification capabilities [15].

Research may continue. First, create UCON administration models such as attribute management, administrative policies, etc. UCON is attribute-based and must acquire and maintain attributes synchronize statically. This article addresses post requirements and post circumstances under the administration model. If a subject fails to complete a duty after access, a security administrator must take compensating steps in line with their policy. The UCON model presented is a next-generation access control system since it contains several new ideas, unlike RBAC and ABAC. This definition defines a topic as a system entity with a set of attributes and capabilities. All objects need characteristics. Objects are accessible to subjects. Based on rights, a person may provide or refuse access to items. IoT designs cannot fulfill the criteria since their rigorous definitions lack clear examples, their extensive descriptions of how access is achieved are inadequate, and until now, only the conceptual model has been produced.

- **Trust-Based Access Control (TBAC) based solution:**
  A formal trust model with a semantic link between three factors attributes, observation, and recommendation was proposed. TBAC proposes an ABAC-based cloud computing IaaS paradigm. TBAC meets necessary standards in cloud computing, notably cloud IaaS. In this architecture, the trust level changes user permissions. ABAC access control rules also vary by user trust. Finally, the concept permits blacklisting malevolent people for a limited time, enabling them to be pardoned if their trust score improves [16].
  Open Stack-based private cloud architecture installs TBAC on a separate VM. The testing findings show that TBAC can analyze access requests within appropriate and acceptable processing times based on the final trust level calculation and communication between TBAC and some of the expected OpenStack services. The ultimate trust level can be estimated at 200 ms under harsh circumstances and with huge traffic overhead, while TBAC's communication overhead with Keystone, Nova, and Neutron are modest. TBAC works and scales in many situations. This study will add additional trust calculation elements.

  Users' trust levels are taken into consideration to dynamically alter their permissions based on their trust level. This paper is primarily focused on providing a foundation for granting access and that foundation is trust. Whenever access control decisions are made, trust is taken into account. Among the three components of trust are attributes, observations, and recommendations, along with semantic relationships among them. The framework is based mainly on the cloud. Additionally, the trust calculation process should incorporate more factors that make the model more effective [3].

- **Capability-Based Access Control (CBAC) based solution:**
  Capabilities give rights to capability-based access control (CapBAC). Capability is the ability to access a computer system entity or object using a token, ticket, or key [17]. The Access Control Matrix (ACM), introduced by Lampson years ago, outlines what will be accessible and who will access it. This ACM has ACLs and capability-based access controls. Unlike capability-based access control, ACL discovered various security risks, including the confused deputy issue. ACL is centralized, cannot accommodate numerous granularities, is not scalable, and has single points of failure.

  Many large-scale IoT initiatives utilize it. ACMs and IoT suffer from using capability-based paradigms. Distributed systems like the IoT must secure resources and data. There are no scalable, manageable, effective, and efficient authorization frameworks to support distributed systems with many services or the dynamicity and scalability needs of IoT contexts that may involve an unbounded number of sensors, actuators, and related resources, services, and subjects, as well as a variety of short-lived, unplanned, and dynamic interaction patterns. Scalable, intelligible, controllable and easy-to-use procedures are needed as more end-users utilize smart devices like smartphones and smart home appliances. This paper's capability-based access control system lets enterprises or individuals restrict access to services and information. The system allows rights delegation and customization. The European FP7 IoT@Work project is developing this method to manage shop floor access to certain of its services [17].

Among the access control methods used in IoT environments, CBAC is considered to be a realistic alternative. In this model, privileges may be granted to entities that possess the stated capability. It is based primarily on the theory of capabilities. Among its many appropriate features, CBAC provides some flexibility, ease of use, and the least privilege principle, making it more suitable to adapt to future internet requirements. However, even though this framework offers relatively more distribution and flexibility than its preexisting models, during the decision-making process it does not consider context, a crucial factor. Revocation and capability propagation are two of the main limitations of conventional CBAC. Mobile device usability is another concern.

- **Smart Organization Based Access Control (SmartOrBAC) based solution:** The IoT has changed our view of the Internet to include smart items in our personal areas. Access management has been crucial to the development of IoT since data breaches and unauthorized access to data and physical equipment might greatly disrupt our everyday lives [18].

  This paper proposes SmartOrBAC, a security and performance-based authorized access paradigm. This concept enhances and adapts OrBAC to IoT contexts. This technique addresses collaboration by splitting the issue into functional levels and distributing processing costs across restricted and less constrained devices. Despite its size, the model adds nothing to standard ACMs.

  SmartOrBAC is an access model built for the IoT environment that uses abstraction layers to make use of a comprehensive understanding of the real-world IoT paradigm. Smart services need real-time contextual information for decision-making. Thus, OrBAC's context notion was extended to IoT. The model has been enhanced with particular collaboration methods to apply the same OrBAC security policy for both local and external access since users belonging to one organization require dynamically access to resources owned by other organizations. SmartOrBAC simplifies and enhances security policy administration. Improve the SmartOrBAC model and execute a validation study to determine its applicability, validity, and practicality. OrBAC-based secure authority delegation may link the end device and RAE/CAE for more dynamic communication. This study also considers privacy upgrades other than pseudonyms and anonymous claims.

IoT is broken down into four layers in SmartOrBAC: One constraint layer, one less constraint layer, one organization layer, and one collaboration layer. In SmartOrBAC splits the problem into various functional layers, which are then allocated with a certain processing cost among constrained and less constrained devices, while keeping in mind a collaborative aspect in parallel. In spite of the fact that this model offers more flexibility, scalability, and fine-grained access policies, its security policies are extremely complex.

- **Pervasive Based Access Control Model (PerBAC) based solution:** The IoT is a worldwide sensor network that links physical and virtual devices to communicate, utilize data, and take physical action. Security challenges are already endangering this paradigm and need effective IoT-specific solutions. This paper covers the essentials. A pervasive-based ACM (PerBAC) for IoT access control (AC).

  This proposal defines PerBAC as a decision-making algorithm, abstract entity idea, and cooperation aspects for numerous organizations. These qualities are perfect consumers of IoT data from the real world and allow effective access control choices based on dynamic rules and entities. IoT research is becoming complex. It has become a massive sensory network with actuation capabilities that are eliminating the physical-virtual split. It has also created new security issues, particularly with the correct AC model for IoT. The real-time IoT paradigm was described from several viewpoints to show how it has grown over the previous two decades and is speeding up and incorporating more smart things [23]. A security assessment of IoT platforms and AC for IoT followed. The study then analyzed the pros and cons of the most common AC models in IoT settings and introduced the PerBAC model [19].

  Describe the four pillars' IoT environment needs, then PerBAC's components, layers, and algorithms. This paradigm may also be used to decentralize structures via cooperation. Simultaneous access in PerBAC causes mild overflow at the code node. DoS attacks are threshold overflows.

- **Transaction-Based Access Control (TBAC) based solution:** The Internet of Things (IoT) has gained greater attention and developed rapidly due to the increase in the number of intelligent devices. Using existing network infrastructure, it enables intelligent devices to share data between the real and virtual worlds. IoT systems, however, face new security challenges and risks because of their complex and large-scale network structure. Considering their complicated access management and lack of credibility due to centralization, traditional access control technologies are not suitable for implementing access control into IoT systems to ensure data security. The paper proposes a novel attribute-based access control scheme for IoT systems, which greatly simplifies access management [20].

The use of blockchain technology can prevent single points of failure and data tampering. For IoT devices, the access control process has also been optimized to meet the needs of high efficiency and lightweight calculation [22]. According to security and performance analysis, the scheme can resist multiple attacks and be efficiently implemented in IoT systems. Blockchain technology, however, has been used only to distribute attributes and avoid data tampering and single points of failure. Due to the high number of attributes in the underlying system, the computational overhead is significant. In terms of storage overhead, session keys are proportional to the number of participants within the network, so scalability might be a problem [22] (Table 1).

Table 1. A comparison of access control models

AC Model	Contributions	Advantages	Limitations
Role Based Access Control (RBAC) [8]	Allows users to access resources according to their roles	while dealing with the distribution of competencies when time and location vary	Access control on an IoT environment is not scalable or flexible
Organization Based Access Control (OBAC) [9]	Based on a structured group of active units known as an organization	Derived from abstractions of entities	Too complicated to implement in the IoT
Attribute Based Access Control (ABAC) [12]	Decision-making relies on attributes	To address dynamic propagation issues	Linking sensor data to attribute values is crucial
Usage Control Based Access Control (UCON) [14,15]	Consists of eight integral components in the form of usage context	Mutable attributes and Authorization are handled dynamically	Definition is not precise
Trust Based Access Control (TBAC) [16]	A key concept is trust level	Evaluation within a reasonable and acceptable time frame	Cloud-based rather than IoT-focused
Capability Based Access Control (CBAC) [17]	Based on the concept of capability	More flexible and distributed than earlier models	Aimed at mobile devices
Smart Organization Based Access Control (SmartOBAC) [18]	Provides context to match IoT requirements	Flexible, scalable, and fine-grained	Complex policy definition
Pervasive Based Access Control (PBAC) [19]	Layers, Attributes, and Matching functions	Proactive, dynamic, large-scale adaptation	Decentralized architecture yet to be implemented
Transaction Based Access Control (TBAC) [20]	A token is managed through a transaction	Token management that is noncentralized and protected	Significantly slow response times

6 Open Research Challenges

Access control systems have been the subject of a significant amount of study and innovation. Several models have already been implemented into functioning systems in the real world. The advancement of technology related to the Internet of Things has led to the thorough integration of information resources for a variety of applications. ACMs and methods need to take into account aspects of the IoT such as the heterogeneity of nodes, open settings, and the collaborative use of resources by many parties [23]. Despite the existence of these problems, a significant number of research efforts have been directed toward the development of new models and methods for allowing access on a finer scale to the resources of IoT systems. Despite this, there are a lot of significant problems that need to be solved.

- **Conflicts in policy due to different authorizations:**
  Many RBAC-related concepts use interpersonal ties as a criterion for access determination; nevertheless, resources are presumed to be held by a single entity, and multiparty sharing is not taken into consideration. Many of the ABAC-related approaches put up an easy solution to this problem, such as restricting access to situations in which all parties involved have given their approval. More work has to be placed into resolving policy conflicts generated by various authorizations to enhance the automation of policy composition and conflict resolution. This will allow for more efficiency.
- **Policy Conflicts Occurring in Multiparty Relationships:**
  The IoT search environment presents this kind of policy conflict problem because of its unique characteristics. The policies of different agents are constrained in the process of integrating multiparty access control policies. The owner of a resource may impose different restrictions on its use. These constraints could lead to several different access control decisions for each resource. Access control decisions can be tailored to the requirements of individual users. These decisions may, however, conflict with each other. It is therefore urgent to find a way of quickly and dynamically selecting and adjusting access control decisions for different users.
- **IoT Security Modeling Evaluation:**
  During the process of IoT search, it is necessary to balance quality, security, and efficiency. As the Internet of Things develops at a rapid rate, more attention is being paid to security. Many other similar complex security problems have been successfully solved with modeling and simulation (MS) in the past. MS methods and tools are also appropriate for resolving IoT problems since IoT devices have unique addresses and communicate using standard protocols. Despite this, we have little data on how IoT security search is modeled and evaluated.
- **Security and Authentication of Physical Devices in the Internet of Things:**
  In the realm of industrial control security and the Internet of Things, there are a number of authentication techniques that may be used to link cloud platforms with sensing instruments in real-time. In most cases, it is not feasible

to provide assurances on both the effectiveness and the safety of these procedures at the same time. Therefore, it is essential to place a greater emphasis on the technology of device authentication and anonymity protection in order to guarantee the dependability, privacy, and availability of data sources.

7 Conclusion

In the present study, a comprehensive survey on ACMs and policies for the Cloud-Enabled Internet of Things is conducted. The core focus lies on the interconnections and relationships between varying models tailored for Cloud-Enabled Internet of Things, assessing the benefits and drawbacks of each. As per the literature analysis, a multitude of models have been devised and developed to facilitate access control in the IoT paradigm. Recognizing the distinctive needs of IoT, various shortcomings of prevalent access control are brought to light. The study also ventures into exploring the advantages and limitations of existing access control solutions from an IoT viewpoint. The provided table conclusively demonstrates that no single model integrates features such as time response, scalability, adaptability to IoT networks, and fine-grain access control into a singular architecture. With IoT security emerging as a prime focus for contemporary researchers, numerous publications point towards security and privacy issues in IoT. Owing to the staggering number of IoT devices and their inherent heterogeneity, traditional access control techniques prove challenging to manage effectively. This review uncovers pivotal studies in the field, providing intricate details on topics attracting significant academic attention and elucidating access control requirements within the context of IoT cloud computing.

References

1. Hassanalieragh, M., et al.: Health monitoring and management using Internet-of-Things (IoT) sensing with cloud-based processing: opportunities and challenges. In: 2015 IEEE International Conference on Services Computing, pp. 285–292. IEEE (2015)
2. Khan, R., Khan, S.U., Zaheer, R., Khan, S.: Future Internet: the Internet of Things architecture, possible applications and key challenges. In: 2012 10th International Conference on Frontiers of Information Technology, pp. 257–260. IEEE (2012)
3. Islam, S.M.R., Hossain, M., Hasan, R., Duong, T.Q.: A conceptual framework for an IoT-based health assistant and its authorization model. In: 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC), pp. 616–621. IEEE (2018)
4. Sandhu, R.: Rationale for the RBAC96 family of access control models. In: Proceedings of the First ACM Workshop on Role-Based Access Control, pp. 9-es (1996)
5. Thomas, R.K., Sandhu, R.S.: Task-based authorization controls (TBAC): a family of models for active and enterprise-oriented authorization management. Status and Prospects, Database Security XI (1998)
6. Karataş, G., Akbulut, A.: Survey on access control mechanisms in cloud computing. J. Cyber Secur. Mobility **7**(3), 1–36 (2018)

7. Goudarzi, M., Ilager, S., Buyya, R.: Cloud Computing and Internet of Things: recent trends and directions. In: Buyya, R., Garg, L., Fortino, G., Misra, S. (eds.) New Frontiers in Cloud Computing and Internet of Things. Internet of Things. Springer, Cham (2022). https://doi.org/10.1007/978-3-031-05528-7_1
8. Sandhu, R.S.: Role-based access control. In: Advances in Computers, vol. 46, pp. 237–286. Elsevier (1998)
9. Kalam, A.A.E., et al.: Organization based access control. In: Proceedings POLICY 2003. IEEE 4th International Workshop on Policies for Distributed Systems and Networks, pp. 120–131. IEEE (2003)
10. Liu, M., Yang, C., Li, H., Zhang, Y.: An efficient attribute-based access control (ABAC) policy retrieval method based on attribute and value levels in multimedia networks. Sensors **20**(6), 1741 (2020)
11. Hu, V.C., et al.: Guide to attribute based access control (ABAC) definition and considerations (draft). NIST Spec. Publ. 800-162 (2013)
12. Ye, N., Zhu, Y., Wang, R., Malekian, R., Lin, Q.: An efficient authentication and access control scheme for perception layer of Internet of Things. Appl. Math. Inf. Sci. **8**(4), 1617 (2014)
13. Kaiwen, S., Lihua, Y.: Attribute-role-based hybrid access control in the Internet of Things. In: Han, W., Huang, Z., Hu, C., Zhang, H., Guo, L. (eds.) APWeb 2014. LNCS, vol. 8710, pp. 333–343. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-11119-3_31
14. Zhang, X., Parisi-Presicce, F., Sandhu, R., Park, J.: Formal model and policy specification of usage control. ACM Trans. Inf. Syst. Secur. (TISSEC) **8**(4), 351–387 (2005)
15. Park, J., Sandhu, R.: Towards usage control models: beyond traditional access control. In: Proceedings of the Seventh ACM Symposium on Access Control Models and Technologies, pp. 57–64 (2002)
16. Riad, K., Yan, Z.: Multi-factor synthesis decision-making for trust-based access control on cloud. Int. J. Coop. Inf. Syst. **26**(04), 1750003 (2017)
17. Gusmeroli, S., Piccione, S., Rotondi, D.: A capability-based security approach to manage access control in the Internet of Things. Math. Comput. Model. **58**(5–6), 1189–1205 (2013)
18. Bouij-Pasquier, I., Ouahman, A.A., El Kalam, A.A., de Montfort, M.O.: SmartOrBAC security and privacy in the Internet of Things. In: 2015 IEEE/ACS 12th International Conference of Computer Systems and Applications (AICCSA), pp. 1–8. IEEE (2015)
19. El Bouanani, S., El Kiram, M.A., Achbarou, O., Outchakoucht, A.: Pervasive-based access control model for IoT environments. IEEE Access **7**, 54575–54585 (2019)
20. Zhu, Y., Qin, Y., Gan, G., Shuai, Y., Chu, W.C.-C.: TBAC: transaction-based access control on blockchain for resource sharing with cryptographically decentralized authorization. In: 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC), vol. 1, pp. 535–544. IEEE (2018)
21. Chatterjee, S., Das, A.K.: An effective ECC-based user access control scheme with attribute-based encryption for wireless sensor networks. Secur. Commun. Netw. **8**(9), 1752–1771 (2015)
22. Srivastava, S., Chaurasia, B.K., Singh, D.: Blockchain-based IoT security solutions. In: Distributed Computing to Blockchain, pp. 327–339. Academic Press (2023)
23. Nižetić, S., Šolić, P., Lopez-de-Ipiña Gonzalez-De, D., Patrono, L.: Internet of Things (IoT): opportunities, issues and challenges towards a smart and sustainable future. J. Cleaner Prod. **274**, 122877 (2020)

Fog Computing in the Internet of Things: Challenges and Opportunities

Iqra Amin Shah[1](✉), Mohammad Ahsan Chishti[2], and Asif I. Baba[3]

[1] Department of Information Technology, School of Engineering and Technology, Central University of Kashmir, Kashmir, India
iqraamin06@gmail.com

[2] Department of Computer Science and Engineering, National Institute of Technology Srinagar, Kashmir, India
ahsan@nitsri.ac.in

[3] Department of Computer Science and Engineering, University of North Texas, Denton, TX 76207, USA
Asif.Baba@unt.edu

Abstract. The expansion of the Internet of Things (IoT) has made it possible for numerous widespread objects to connect to one another and communicate with one another, leading to unprecedented data releases. However, regardless of the fact that cloud computing has been a useful tool for processing and storing these data, problems like the growing demand for real-time applications and the constrained availability of network bandwidth cannot yet be resolved solely through the use of cloud computing. As a supplement to the cloud solution, a new approach to computing called the fog computing paradigm has been developed. By moving processing, connectivity, and capacity nearer to edge gadgets and end clients and taking cloud computing to the network's edge, fog computing aims to increase low latency, activity, data traffic, reliability, and privacy. The present paper discusses the framework of the fog computing model and presents a literature survey of various works that is carried out on fog computing. It also covers the current problems and difficulties in fog computing and opportunities for research in the area of Fog computing for the Internet of Things.

Keywords: Internet of Things · Fog Computing · Edge Computing · Cloud Computing

1 Introduction

With the increase in the data produced by the internet of things (IoT) devices, different entities, including people, things, and, machines are connected in a global village anywhere at any time. A vast amount and variety of data are being produced. According to the survey by Cisco, "there are more than 30 billion devices that will be connected to the Internet by 2025" [1].

Published by Springer Nature Switzerland AG 2024
D. Puthal et al. (Eds.): IFIPIoT 2023, IFIP AICT 684, pp. 198–211, 2024.
https://doi.org/10.1007/978-3-031-45882-8_14

The Cloud computing paradigm is a paradigm that has storage, computational and communicational capabilities. The data formed by IoT devices is prepared and stored in the cloud. “Infrastructure as Service (IaaS)”, “Platform as a Service (PaaS)”, and “Software as a Service (SaaS)” are all service providing models that the cloud can offer. IaaS offers resources that have been virtualized: including computers, storage, and networking. It is used by Network Architects. PaaS offers a Software platform for the formation, consumption, and management of services. It is used by application developers. The SaaS offers end users and other applications software and merged services. It is mainly used by end users. It has high computation power and storage capabilities. Although, as Cloud Computing is not a distributed computing architecture majority of operations are performed in the cloud. Because of this, all the data needs to transfer to the cloud. Since there is a movement of data distant from the edge gadgets it results in an increase in network bandwidth. Due to this, long latency occurs [2].

The delay in cloud computing, which is caused by increasing bandwidth is intolerable. Also, there is no need to transmit all data to the cloud as some decisions can be made nearby without the intervention of the cloud. Because these challenges are due to the volatile enhance of IoT devices only using the cloud to solve issues with network capacity, delay, and security is not a solution. So, to overcome these limitations fog computing has been suggested as a way to employ the computer tools close to the users. This is a supplement of cloud computing approach nearer to the devices that produce and senses the data [3]. In other words, we can say Fog computing is an association of cloud computing and the IoT. These devices are connected to the network anywhere at any time. Fog Computing is a decentralized computing framework in which different computing resources and devices are connected to provide the service of cloud computing at the edge. It pools the local resources for processing, connectivity, management, and storage. Fog computing strives to be better effectiveness and diminish the quantity of data that needs to be delivered to the cloud for preparing, analyzing, and archiving. In order to diminish network traffic and latency, sensors will send data to edge devices of network for handling and temporary storage rather than to the cloud [4]. In addition to improving efficiency, this can also improve security.

Applications that are time-sensitive including multimedia and notifications can respond quickly using fog computing.

1. It supports the collection of data from various devices. For instance, it can aggregate information from several sensors relevant to healthcare.
2. Sensitive data, such as medical records, user whereabouts, and other private information are protected and secured by it.
3. By screening the data before transmitting it to the main network, it avoids pointless communication.
4. Due to its proximity to the user and ability to gather additional information about them, it offers context and location-aware services.

This paper reviews and summaries the fog computing, applications, and difficulties. The idea of fog computing is briefly explored in this work.

2 Architecture of Fog Computing

Different literature has suggested a various number of architectures for fog computing, many of which share some similarities. But none of the architecture has yet achieved standardization. A key research area is the reference model of fog computing architecture. Several architectures for fog computing have been presented in recent years. Recently, the Open Fog Consortium said that they were working to standardize the architecture they had suggested. The majority of the suggested structures were derived from a simple 3- layer framework [2]. Fog computing creates a layer of fog between end users and the cloud to extend services of cloud to the network edge. The tiered architecture of fog computing is shown in Fig. 1. Three levels make up this tiered architecture for fog computing– the cloud, the fog and the terminal layer [2].

1. The cloud layer: This layer offers a variety of application services, including smart home, smart factory, and smart transportation, and is made up of several powerful servers and storage systems. It provides strong processing and storage abilities that allow for significant computation, in- depth analysis, and long-term data storage. Yet, not all processing and storage operations use the cloud, unlike conventional cloud computing architecture. To maximize the use of the cloud resources, the cloud core components are effectively scheduled and controlled in accordance with demand-load [1].
2. The fog layer: This layer is situated at the network's outermost point. Numerous fog nodes, such as entry points, central stations, particular fog servers, routers, gateways, switches, etc., comprise the fog computing layer. These fog nodes are located widely between the cloud and end devices. They may be stationary at a specific area or travelling with a carrier. To acquire services, the end devices can easily connect to fog nodes. They are equipped to process, transmit, and transiently store the detected

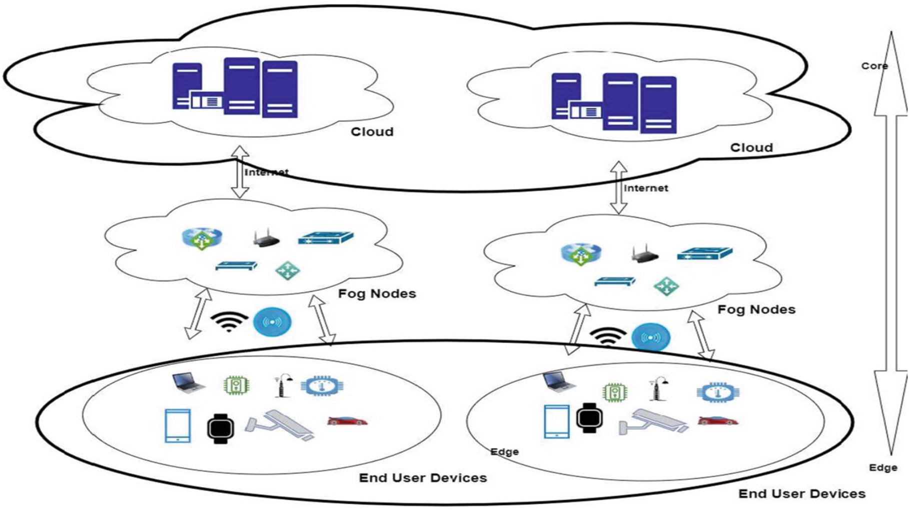


Fig. 1: Architecture of Fog Computing

data that they have received. In the fog layer, proper analysis and latency-sensitive applications are possible. Additionally, the fog nodes are liable for interacting and working with the cloud to get more potent computation and memory capabilities. They are connected to the cloud data center via an internet protocol core network.

3. The terminal layer: The layer is the nearest to the customer and the real world. It consists of a variety of IoT devices, such as detectors, cell phones, intelligent transportation systems, swipe cards, scanners, and much more. Even though smart cars and mobile phones have powerful computers, we only use them as smart detecting devices in this situation. In general, these devices are widely dispersed spatially. They are in control of capturing feature data from actual objects and sending it to a higher layer for storage and processing.

3 Specifications and Benefits

1. Real-time interactions with low latency: The data generated by detectors and devices is locally acquired by fog nodes at the network edge, where the data is analyzed and saved by network edge gadgets in regional networks. It offers quick, excellent customized solutions driven by end users and considerably decreases data transit across the Internet. In order to enable low latency and fulfill real-time interaction requirements, particularly for delay-sensitive or applications that are time-sensitive.
2. Reduces Bandwidth: To prepare and keep data between end nodes and a standard cloud, fog computing expands compute and storage capabilities to the network edge. Some computation operations are carried out locally, such as data preparation, duplication removal, data cleansing and scanning, and collecting information.
3. Most relevant data does not require to be sent through the Internet, and only a small portion of it is actually transferred to the cloud. Compared to the conventional cloud computing approach, which required submitting raw facial images to the cloud, fog computing significantly lowered network traffic and reduced bandwidth.
4. Supports mobility: In fog computing applications, there are a variety of portable devices (such as cell phones, automobiles, and smart watches) that contribute to the frequent spatial movement at the terminal layer. However, some end devices including surveillance cameras, stay fixed. In the same way, a platform for computing resources that is movable or static can be a fog node in a fog layer. For fog computing to work, continuous handheld device connection is essential. Various mobile gadgets can also directly communicate with one another. The data does not have to be received by the central station or even the cloud. End devices or intermediaries must analyze the huge volumes of data generated by the Internet of Things in order to fully realize portable analysis of data so that a greater choice of services may be provided.
5. Decentralized data analysis and geographic distribution: In contrast to cloud computing, which is more concentrated, fog computing solutions and applications support geographically distributed provision. It consists of a huge number of extensively disseminated nodes that can monitor and ascertain the positions of end devices in an effort to assist portability. Because of the dispersed design of fog computing, data analytics can take place close to the consumer rather than being processed and

stored in centralized servers far from end users. This attribute can be used to facilitate quicker massive data processing, better services based on location, and a more robust immediate-time ability to make decisions. The objective of IoT and ubiquitous computing environment is to link and integrate various ubiquitous objects. Not only are there a tone of these things, but they are also widely dispersed. Geographical dispersion and decentralized data analytics have the ability to successfully meet the afore mentioned requirements.

6. Heterogeneity: Fog nodes are typically deployed in a number of environments and exist in a range of form factors, including physical nodes and virtual nodes. High-performance computers, edge routers and switches, entrances, access points, central stations, and other components are commonly included. These physical platforms run different operating systems (OS), load diverse software programmes, and have differing degrees of computing and storage capacity. As a highly virtualized platform, fog computing allows for the employment of some practical nodes, such as practical network and computation nodes. Fog nodes are hence heterogeneous.
7. Interoperability: Fog nodes and end devices are typically deployed in multiple contexts because to their heterogeneous nature, which allows them to come from different suppliers. To handle a broad variety of services and smoothly support some services, Fog computing should be able to interact and work together with a broad range of sources. For instance, federated services across domains are necessary for the streaming service that fog computing supports.
8. Information security and confidentiality protection: Open-access services are hosted using fog computing. Consequently, it provides unique benefits for data security and confidentiality protection. It can first secure data using encryption and remoteness. To safeguard the security of sensitive confidentiality data, fog nodes include access management procedures, encryption techniques, and separation measures. Second, it can prevent the dangers associated with system upgrades.
9. Minimal energy usage: Fog nodes in the fog computing framework are purely scattered. Due to the concentration, it doesn't generate much heat and won't require a separate cooling system. Additionally, mobile nodes' best energy management policies and short-range communication mode clearly cut back on energy used for communication. As a result, there will be less electricity used, more energy saved, and lower costs.

4 Internet of Things

In 1999, Kevin Ashton first used the phrase "internet of things." As a result of advancements in computing, the internet, and the rate at which data is generated by smart gadgets, he thinks that the "things" part of how we interact and live in the physical world around us requires significant rethinking. The Internet of Things (IoT) is a network composed of real objects, devices, machines, structures, and other things that have been combined with technology. This network allows these things to gather and transfer information. Through the use of existing network infrastructure, things can be detected and remotely controlled via the Internet of Things. This direct integration of the real world and computer-based systems leads to increased effectiveness, accuracy, and financial gain. When loT is enhanced with sensors and actuators, the technology is categorized as a cyber-physical system, a more generic category that also includes grids, smart homes, intelligent transportation, and smart cities. Each object has an embedded computing system that makes it uniquely identifiable, but it can still communicate with other things using the current Internet infrastructure. While employed at Auto-ID Labs (formerly known as Auto-ID centers, alluding to a global network of Radio- frequency identification (RFID) connected devices), the entrepreneur Kevin Ashton initially invented the phrase in 1999.

The Internet of Things (IoT) is typically anticipated to provide improved connectivity of hardware, software, and services that extends beyond machine-to-machine (M2M) communications and spans a range of protocols, domains, and applications. It is anticipated that the interconnection of these embedded devices, including smart objects, would enable sophisticated applications like a Smart Grid and expand to areas like smart cities, ushering in automation across practically all industries. In the perspective of the Internet of Things, "things" can refer to a extensive collection of devices, including devices for heart monitoring, biochip transmitters on live stocks, electric oysters in coastal waters, sensors equipped cars, DNA analysis devices for natural, food, parasite monitoring, or field operation tools that aid firefighters with search and rescue efforts. These gadgets use a variety of already available technologies to acquire important data, which they then autonomously transfer to other devices. Examples available right now include Wi-Fi-enabled washers and dryers and smart thermostats. Before the Internet was even called the Internet, manufacturers were already connecting products to it. Web servers were being incorporated into embedded goods by the mid-1990s. For more than 15 years, current M2M manufacturers have been incorporating Internet-connected systems into fleet management, alarm systems, high value asset tracking, and other applications. Even though some of these M2M systems are based on industry-standard protocols, they are difficult to construct. However, when more potent processors are put into the end nodes and since these processors enable high level operating systems and languages, the platform may utilize intelligent frameworks, integrating M2M systems is becoming easier. These systems are often controlled by a network operations centre (NOC) and connected to high-end business service layers. Although both the industrial and consumer situations are interesting, because they involve several vertical separate systems, deployment is not made any easier. Although the OS and protocols used by the systems are same, the communications layers differ. In order to facilitate easier cross-application integration, each also makes use of open application programming interfaces (APIs) without a horizontal link.

To progress the performance of IoT services, the majority of the information produced by the IoT items and gadgets needs to be handled and evaluated in immediately [21]. Fog will deliver cloud connectivity, processing, and capacity services to the network's edge, resolving the problem of real- time IoT device operation and enabling dependable and safe IoT applications [22]. Several IoT applications will benefit greatly from the incorporation of fog computing. The fog enables real- time communication among IoT devices to minimize delay, particularly for critical IoT applications. Extensive sensor networks are a serious problem with the IoT's rapidly rising quantity of devices, which will ultimately number in the hundreds of millions. Fog computing also has the ability to handle these networks. Numerous IoT services can benefit greatly from fog computing.

Fog computing can address the following IoT difficulties, as per the M. Chiang and T. Zhang [23]:

a) Latency limitations: The fog is the appropriate resolution to assemble the latency requirements of various IoT applications since it executes all compute operations close to end users, including maintaining and examining data and other time-critical tasks.
b) Network capacity limitations: Fog computing enables multilayer processing of information from the data centre to IoT devices. This allows the handling of data according to the requirements of the application, the available system, and the computer resources. Because of this, the quantity of data that requires to be transmitted to the cloud is minimized, resulting in less traffic across the network.
c) Devices with limited resources: Fog computing enables devices with few features to do tasks that demand a lot of computational power but cannot be transmitted to the cloud. As a consequence, device intricacy, lifetime expenses, and electrical usage may all be decreased.
d) Continuous services: Even with irregular network connectivity to the cloud, fog can continue to operate independently to guarantee continuous services.
e) IoT security difficulties: Devices with limited resources have fewer security features, as an outcome fog computing functions as a medium for these devices for updating their operating systems and privacy settings. Additionally, the security status of adjacent devices can be checked using the fog.

This discusses the convergence of fog computing with the IoT. The next section gives an overview of related work that has been carried out in different papers.

5 Literature Survey

The purpose of this Section is to demonstrate how the fog computing has been described in various contexts.

Jabril, et.al [5] suggested the architecture paradigm of fog computing. The basic components as well as the requirement for uniform data were made clear. The potential adaptation and applications needed for this model were used to illustrate the use case scenario for the Flood Warning System. They recognized service operation, runtime implementation, and thing collaboration as the study problems in fog computing.

Arif, et.al [6] discussed the futility of transferring the gigantic amount of data produced by IoT devices and sensors to the data centre in the cloud for activities that need to be provided immediately. To give a good understanding of the realistic domains where fog computing is useful, examples of applications and how they use the technology were presented.

Fog can be deployed using Private, Public, Community, or Hybrid fog models. Depending on their hardware platforms fog Nodes were classified into fixed and dynamic fog nodes. The distribution model was given via fog computing in two different hardware and software setups. The service models of fog computing were additional classified as

"Fog- Software as a Service" (Fog-SaaS), "Fog-Platform-as-a-Service" (Fog-PaaS) [7], and "Fog-Infrastructure-as-a- Service" (Fog-IaaS). Platform designers would benefit more from this recommended study.

The concerns in relation to structure, service, and security were discussed by Redowan, et.al [8]. Utilization of different processor types in various fog environment infrastructure components from the edge and the core network presented a variety of issues. The difficulties encountered while implementing large-scale applications in a Fog Node with restricted resources were also made clear. Concerns about protecting privacy in systems that are substantially distributed and the importance of developing authenticated systems were also covered. With the collection of already published works in fog computing, a fog computing taxonomy is offered. Based on the ways taken to deal with the mentioned difficulties, the taxonomy indicated how fog computing analysis was done.

According to Mohammed et al. [9], the fog computing is a supplementary means to cloud computing. The system must manage a significant volume of time-sensitive data and be in need of a quick review report since the research world of today is driven to build product-service-systems rather than products, mainly in the situation of Industry 4.0. Throughout this study, they outlined the advantages of combining cloud computing and fog computing.

Schahram, et.al [10] focused on Edge computing and fog computing. Based on each computing paradigm's unique traits and use cases, they discussed about both the cloud as well as fog paradigms. They also discussed upcoming difficulties such as network administration, resource management, and security and privacy. They addressed the requirement for social adaptability in the study solution. The smart city illustration and its uses in fog computing environment customization were stated clearly.

According to Abdul Rahman, et.al [11] fog computing has been compared to a bridge that has been established for the purpose of bridging the separation between remote cloud servers and end user devices. Fog is a suitable paradigm for many IoT functions because it offers a several advantages, such as improved security, lower bandwidth use, and decreased latency. However, there are definitely numerous security and confidentiality risks for fog devices which are positioned at the edge of the Internet. The author of this paper discusses security and confidentiality concerns in IoT contexts and suggests a means for IoT device safety improvement using fog computing to enhance the dissemination of details on certificate suspension among them.

Javier, et.al [12] explored the various justifications for why the cloud computing paradigm can't satisfy specific needs, such as low latency, context dependent and mobility support, which are essential for a number of applications. The different paradigms, including "mobile cloud computing (MCC)", "mobile edge computing (MEC)", and "fog computing", have arisen in past the few years to satisfy the stated needs, with fog computing making a significant contribution by acting as an edge node between IoT and cloud. Additionally, there are similarities among the edge paradigms; however, the majority of recent study is fragmented, and no tactics have been looked into. This is particularly correct in the security industry, as most evaluations only pay attention to one edge while ignoring the others. This paper's major objective is to comprehensively and thoroughly analyze the security risks, difficulties, and procedures present in all edge paradigms while stressing on opportunities for collaboration and cooperation. The authors of the research claim to demonstrate how all cutting-edge paradigms should take advantage of paradigm developments. Jianbing Ni. et.al [13], examined about fog computing in IoT. With the help of the IoT billions of devices can be connected and used for things like smart cities, home automation, and environmental surveillance through the process of gathering and transferring data across linked objects. Despite having mentioned qualities, IoT also has additional aspects that are essential for specific IoT applications, such as smart grid. Typical characteristics include low latency, location responsiveness, and geographic dissemination. The introduction of fog computing enables these features. By utilizing fog computing in IoT, processing, storage, and networking capabilities are expanded to the network. On the other hand, it is implied that consumers may experience a number of security and privacy difficulties. We examine the capabilities of fog computing architecture. Further, studies have been done on immediate services, temporary capacity, distribution of data, and independent computation, all of which are key functions of fog nodes. Every IoT application related to fog is tested using various fog activities. Threats to IoT's safety and confidentiality are then mentioned. A new architecture provides approach for security and privacy issue in the IoT application for fog computing.

Bala, et.al [14] mentioned the scope of fog computing and its hierarchical design in detail. In an effort to enable academics to concentrate on fundamental Fog concerns, they also reviewed significant Fog applications and the significant hurdles that must be addressed in order to fully utilize fog computing. They have highlighted some holes in the literature, such as the lack of standards in fog computing, which could serve as future topics for research.

Pengfei, et.al[15] provided a detailed analysis of the architecture, important technologies, applications, and open challenges in detail. Additionally, the similarities and differences of fog with cloud computing and edge computing are also discussed. The major technologies, such as those used in computation, interaction, and capacity, as well as identification, resource planning, security, and confidentiality protection, are then briefly discussed to show how to enable their deployment and use in detail. To better clarify fog computing applications, a number of application examples are discussed, including those related to health care, wearable technology, central nervous system interface, gaming, IoT, and smart surroundings. Finally, certain difficulties and open problems are discussed. These problems include security and privacy, programming environment, and energy usage. To support the growth of IoT and big data, fog computing will act as a more bright and environmentally friendly computing paradigm.

6 Current Technologies in Fog Computing

The fast-evolving realm of fog computing hosts several cutting-edge technologies currently applied within its ecosystem – enabling businesses to harness this innovative concept further.

In this sense, one key area comprises utilizing edge devices like Raspberry Pi boards that offer highly compact sizes alongside low-power consumption rates when operating either as gateways or sensor nodes. Another popular option is the NVIDIA Jetson processor lineup specifically designed for AI and deep-learning-driven applications occurring at edges' proximity beside Intel NUCs offering decent processing power valuable within fog nodes or constituent gateways.

Additionally, communication and networking play critical roles herein; thus featuring protocols like MQTT (Message Queuing Telemetry Transport) tailored explicitly to cater to constrained devices alongside unconventional/more unreliable circuits.

CoAP (Constrained Application Protocol) comes to rescue as a specific resource-constrained device protocol ideal for operating over low-power networks. Moreover, LoRaWAN (Long Range Wide Area Network) emerges as an essential networking protocol that benefits wireless IoT deployments with outstanding long-range capabilities.

Lastly, when it comes to data processing and analytics duties, several high-performing tools desire a mention. For instance, Apache Kafka serves as an efficient distributed streaming engine granting the ingestion, storage as well as efficient processing at voluminous rates of real-time data streams.

Additionally, there's Apache Spark – an open-source distributed computing system providing in-memory machine learning/analytics task execution abilities on large-scale datasets with ease. Tensor Flow Lite is another notable platform that facilitates the deployment of machine learning models on low-end devices like smart phones - this enables effective implementation of ML algorithms on such devices without compromising performance. Finally, Open CV offers excellent computer vision-based image/video processing using unique algorithms for diverse industry usage domains such as robotics/hospitality/research among many others. Ensuring security and privacy in Fog Computing is of utmost importance. One way to achieve this is by using Secure Shell (SSH). A cryptographic network protocol that enables secure remote access and secure file transfer between fog nodes and gateways.

Another method is to leverage Virtual Private Networks (VPNs) which create an encrypted tunnel over public networks to facilitate secure communication between fog nodes. Trusted Platform Modules (TPMs) provide hardware based security solutions such as secure storage for cryptographic keys, attestation, and secure booting.

Effective orchestration and management play vital roles in the success of Fog Computing. Kubernetes, a container orchestration platform enables the deployment, scaling, and management of applications and services across multiple fog nodes and edge devices. Open Stack provides infrastructure management capabilities for cloud computing platforms while also having the capability of extending its services for managing resources in Fog Computing. Automation tools like Ansible allow configuration management for all components within Fog Computing such as fog nodes, gateways. Infrastructure components ensuring ease of use.

7 Discussion

We can learn various things about fog systems from this literature review. First, compared to conventional cloud systems, fog systems do indeed provide lower latency. Measurements from both simulations and experiments show that large reductions in delay are possible. For real-time applications like IoT apps, this is important. A number of references, including [16–19], and [15] showed this reduced delay. It should be noted that while latency decrease is not automated, the placement of the application elements impacts it. When certain application elements are located in the cloud and others are in the fog, the reaction time may occasionally be worse than if they were all in the cloud. The advantage of lower latency should be emphasized that not all IoT scenarios require it. As an illustration, manufacturing IoT services typically require short delay impulses, although rapid data processing [20].Such systems may not always be able to accommodate the lengthy delays in data transfers to the cloud and their distant analysis. Consequently, we can now move on to the second lesson about traffic reduction across communication channels to the cloud. Fog nodes' local processing uses less bandwidth and speeds up processing. It could prevent the sending of incorrect or irrelevant data to the cloud for handling and/or storage needs purpose.

As a result, the amount of data transmitted is decreased, and the traffic through the system's various strata is also significantly reduced. A reduced amount of traffic is transmitted to the cloud while utilizing fog, according to several references, including [16–18]. [17] Showed a "reduction in the data size of up to 93 percent when employing a fog system", while [18] showed that the "data transported to the cloud is 0.02 percent of the overall size".

It has been demonstrated that fog systems use little energy. Fog systems are notable for their minimal delays, little traffic on the network to the cloud, and low energy consumption. A study of the system's overall energy use reveals that fog computing systems use less energy than cloud computing systems, which signifies reduced costs as discussed in [16].

8 Open Issues and Challenges

1. Security and confidentiality concerns:
   Since fog computing devices are typically deployed in areas without severe protection and supervision, they are susceptible to conventional attacks that may harm the fog device's system to order to carry out deceitful tasks such as data stealing and snooping. Cloud computing security options are plentiful. However, because fog computing devices operate at the edge of networks, these solutions might not be applicable. Fog devices may be exposed to a variety of dangers that do not subsist in cloud computing. Here is a catalog of several well-known assaults that can be made to fog computing.
   a. Man in the middle: The intruder may examine or disrupt communications between fog devices since small devices often lack the capabilities to create reliable communication methods, the man-in-the-middle assault is possible to become a common attack in fog computing.
   b. Authentication: As authentication needs to work to access staff devices physically while the distant verification server connections are down, relying on the cloud's central verification servers is not the ideal solution. Several verification and trust challenges may arise for fog-based devices, such as gateways, that do not present in the normal scenario.
   c. Distributed denial of service: The most difficult security risk facing websites and online services today is known as "distributed denial of service, or DDOS". Fog nodes have limited resources, making it difficult for them to handle many requests

at once. By simultaneously issuing a large number of unnecessary service requirements, fog nodes may happen to swamped for an extended span of time. As a consequence, there are no resources available to host genuine services.

   d. Access control: To satisfy the objectives and resource restrictions at various levels, one can ask how to construct access control via client-fog cloud in fog computing. Access control has established itself as a trustworthy solution for ensuring system security.
   e. Fault tolerance: When specific sensors, connections, service mediums, or applications malfunction, fog computing should continue to offer services normally. Because fog nodes are widely scattered geographically, clients should be able swiftly move to other closest nodes using an acceptable means when the service in a specific region is anomalous.

2. Management and control:
   a. Application-specific provisioning: By offering provisioning based on application, fog computing is anticipated to provide movable apps for crowd sourcing and sensing. A fog network must execute provisioning to set up its infrastructure for operational flexibility and to meet QoS requirements for Fog, such as latency. The mobility of end nodes presents a problem because metrics like connectivity, archiving, compute, and rapidly will change rapidly.
   b. Fog resource management: The cloud computing paradigm is anticipated to be expanded by fog computing to the network's edge. Fog management of resources, like distribution and exploration, is sensitive for application effectiveness. Fog computing allows for the sharing of diverse resources and supported services by both centralized data centers and widely used mobile devices.
   c. Programming platform: A programme built in a particular programming language and running on the cloud performs the computational work in cloud computing, where the framework is visible to the person using it. Programming in such diverse platform is extremely difficult since in fog computing, computation must be performed in client end boundary nodes, which are almost certainly running diverse platform and typically vary from one another. Consequently, a uniform development framework for fog computing is now absolutely necessary. Since fog nodes are often portable devices that constantly switch between networks, fog environments need the capability to vigorously affix and take out nodes. As an outcome, most stream-processing and data- processing platforms lack the capacity and adaptability required for fog computing as their architecture is based on fixed setups relatively than active ones.
   d. Energy management: Given that fog computing systems have a larger number of distributed nodes than cloud computing systems, their expected usage of energy exceeds. In order to build and refine highly optimal cost-effective methods and designs for the fog paradigm, such as effective interaction procedures, computation, and network bandwidth improvement, much work still needs to be done.

9 Conclusion and Future Scope

Fog computing is a fast-processing computing paradigm whose importance is rising quickly because of the IoT and the mobile internet's quick expansion. The fog paradigm drives an increasing number of services out of the cloud and into the network edge by fully using geographically dispersed network edge devices. It successfully meets the needs of immediate time or applications that are sensitive to latency, decreases the volume of network transmission, and considerably reduces the time required for data transfer. It also helps to relieve network capacity bottlenecks. This features the fog computing architectural paradigm for clear comprehension. The literature review reveals that fog computing is a benefit for applications of IoT and the cloud that provide functions with short response times, lower cloud data center energy usage, improved performance, and more. In the case of IoT services, it abruptly reduces the Cloud demand. To support the growth of IoT and big data, fog computing will act as a extra vivid and environmentally friendly computing paradigm. This is an important field of study that will have an impact on academia and business in the future. Taking into account the challenges mentioned, here are some suggestions for future work. To mitigate the vulnerability to man-in-the-middle attacks, researchers can focus on designing robust and secure communication protocols that are specifically designed for fog computing devices. Develop methods and designs to optimize energy usage in fog computing systems, including efficient interaction procedures, computation techniques, and bandwidth utilization. These future research directions aim to address the specific challenges and requirements of fog computing, ensuring better security, efficient management, and improved performance in fog-based systems.

References

1. Evans, D.: The Internet of Things: How the Next Evolution of the Internet is Changing Everything-White Paper (2011). www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf. Accessed 13 Sep 2017
2. Hu, P., Dhelim, S., Ning, H., Qiu, T.: Survey on fog computing: architecture, key technologies, applications and open issues. J. Netw. Comput. Appl.Netw. Comput. Appl. **98**, 27–42 (2017). https://doi.org/10.1016/j.jnca.2017.09.002
3. http://conferences.sigcomm.org/sigcomm/2012/paper/mcc/p13.pdf
4. Wen, Z., Yang, R., Garraghan, P., Lin, T., Xu, J., Rovatsos, M.: Fog orchestration for internet of things services. IEEE Internet Comput.Comput. **21**, 16–24 (2017)
5. Jabril Abdelaziz, M.A., Mcheick, H.: An architectural model for FC. J. Ubiquitous Syst. Pervasive Networks **10**(1), 21–25 (2018)
6. Ahmed, A., et al.: FC Applications: Taxonomy and Requirements (2019). arXiv:1907.11621v1 [cs.DC] 26 Jul 2019
7. Yangui, S., et al.: A platform as-a-service for hybrid cloud/fog environments. In: 2016 IEEE International Symposium on Local and Metropolitan Area Networks (LANMAN), pp. 1-7 (2016). https://doi.org/10.1109/LANMAN.2016.7548853
8. Mahmud, R., Kotagiri, R.M., Buyya, R.: FC: A Taxonomy, Survey and Future Directions. © Springer Nature Singapore Pte Ltd. 2018, Di Martino, B., et al. (eds.), Internet of Everything, Internet of Things (2018)

9. Al Yami, M., Schaefer, D.: FC as a Complementary Approach to Cloud Computing. International Conference on Computer and Information Science (ICCIS), At Jouf University, Al Jouf Region, Kingdom of Saudi Arabia (2019). https://doi.org/10.1109/ICCISci.2019.8716402
10. Dustdar, S., Avasalcai, C., Murturi, I.: Edge and FC: vision and research challenges. 2019 IEEE International Conference on Service- Oriented System Engineering (SOSE). Date of Conference: 4–9 April 2019, Date Added to IEEE Xplore: 06 May 2019, INSPEC Accession Number: 18638357 (2019). https://doi.org/10.1109/SOSE.2019.00023, Publisher: IEEE,Conference Location:San Francisco East Bay, CA, USA
11. Alrawais, A., Alhothaily, A., Hu, C., George, X.C.: Washington University
12. Romana, R., Lopeza, J., Mamboba, M.: Computer Science Department, University of Malaga, Ada Byron building, 29071 Malaga, Spain. bFaculty of Electrical and Computer Engineering, Institute of Science and Engineering, Kanazawa University, Kakuma Kanazawa 920- 1192, Japan
13. Ni, J., Zhang, K., Lin, X., Shen, X.: Securing fog computing for internet of things applications: challenges and solutions. IEEE Communications Surveys & Tutorials **20**(1), 601–628 (2018). https://doi.org/10.1109/COMST.2017.2762345
14. Bala, M.I., Chishti, M.A.: Survey of applications, challenges and opportunities in fog computing. International Journal of Pervasive Computing and Communications. ahead - of-print (2019). https://doi.org/10.1108/IJPCC-06-2019-059
15. Sarkar, S., Misra, S.: Theoretical modelling of fog computing: a green computing paradigm to support iot applications. IET Netw. **5**(2), 23–29 (2016)
16. Krishnan, Y.N., Bhagwat, C.N., Utpat, A.P.: Fog computing - Network based cloud computing. In: 2015 2nd International Conference on Electronics and Communication Systems (ICECS), pp. 250–251 (2015)
17. Gia, T.N., Jiang, M., Rahmani, A.M., Westerlund, T., Liljeberg, P., Tenhunen, H.: Fog computing in healthcare internet of things:a case study on ECG feature extraction. In: 2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing (CIT/IUCC/DASC/PICOM), pp. 356–363 (2015)
18. Tang, B., Chen, Z., Hefferman, G., Wei, T., He, H., Yang, Q.: A hierarchical distributed fog computing architecture for big data analysis in smart cities. In: Proceedings of the ASE Big Data & Social Informatics 2015, New York, NY, USA, pp. 28:1–28:6 (2015)
19. Li, J., Jin, J., Yuan, D., Palaniswami, M., Moessner, K.: EHOPES: data-centered fog platform forsmart living. In: Telecommunication Networks and Applications Conference (ITNAC), 2015 International, pp. 308–313 (2015)
20. Perera, C., Liu, C.H., Jayawardena, S.: The emerging internet of things marketplace from an industrial perspective: a survey. IEEE Trans. Emerg. Top. Comput.Emerg. Top. Comput. **3**(4), 585–598 (2015)
21. Atlam, H.F., Alassafi, M.O., Alenezi, A., Walters, R.J., Wills, G.B.: XACML for building access control policies in internet of things. In: Proceedings of the 3rd International Conference on Internet of Things, Big Data and Security (IoTBDS 2018), Setúbal, Portugal, pp. 253–260 (2018)
22. Ketel, M.: Fog-cloud services for IoT. In: Proceedings of the SouthEast Conference, Kennesaw, GA, USA, pp. 262–264 (2017)
23. Chiang, M., Zhang, T.: Fog and IoT: an overview of research opportunities. IEEE Internet Things J. **3**, 854–858 (2016)

A 2-Colorable DODAG Structured Hybrid Mode of Operations Architecture for RPL Protocol to Reduce Communication Overhead

Alekha Kumar Mishra[1](✉), Sadhvi Khatik[1], and Deepak Puthal[2]

[1] Department of Computer Science and Engineering, National Institute of Technology Jamshedpur, Jamshedpur, India
alekha@gmail.com

[2] C2PS, Department of EECS, Khalifa University, Abu Dhabi, UAE
deepak.puthal@ku.ac.ae

Abstract. The Routing Protocol for low-power and lossy Networks (RPL) is the established standard for packet-level communications in the Internet of Things (IoT). The efficiency of point-to-point (P2P) communications in RPL relies on the mode of operation employed by the network nodes. Hybrid modes of operation (MOP) have gained attention as they combine the advantages of both standard non-storing and storing operation modes. However, existing hybrid MOPs have struggled to achieve a balance between reduced communication overhead and storage overhead. To address this, we propose the application of the 2-colorable graph property to enable a hybrid mode of operation among IoT network nodes. By mapping the two-colorable property to the standard MOPs, we conduct experiments comparing the proposed hybrid MOP with existing approaches. Results demonstrate that our proposed hybrid MOP achieves a significant balance between storing and non-storing nodes, while also exhibiting improved average path length compared to existing hybrid MOPs. This research contributes to optimizing P2P communications in RPL-based IoT networks and highlights the potential benefits of utilizing the 2-colorable graph property in achieving an efficient hybrid mode of operation.

Keywords: IoT · DODAG · RPL · Mode of operations · hybrid MOP · 2-colorable graph

1 Introduction

The IoT comprises almost all the object that are part of our home, vehicles, office, service centers in cities and rural areas [3]. The key component of IoT is its underlying communication system that includes a huge set of communication technologies [10,13]. The unlimited demand of wireless technologies have given rise to a number of wireless technologies for wide range of devices and their

Published by Springer Nature Switzerland AG 2024
D. Puthal et al. (Eds.): IFIPIoT 2023, IFIP AICT 684, pp. 212–224, 2024.
https://doi.org/10.1007/978-3-031-45882-8_15

applications using IoT. The IPv6 over IEEE 802.15.4e TSCH mode (6TiSCH) [4,15] is designed to provide interface between TSCH link layer and IPv6 upper layer protocol stack. The 6TiSCH provides open protocol stack for multi-hop communication. The routing in 6TiSCH is supported by enhanced version of standard RPL protocol. The RPL has been standardized by the Internet Engineering Task Force (IETF) in 2012 [1,14]. The RPL protocol establishes a Destination Oriented Directed Acyclic Graph (DODAG) architecture among the IoT devices in order to facilitate packet communications. The major traffic in RPL are Multi-Point-to-Points (MP2P) type. However, the recent IoT applications demand more kinds of P2P communications [11]. Apart from these two types, the RPL also commonly supports Point-to-Multi-Point (P2MP) communications.

In P2P type communications, each device in a RPL-DODAG operates in two modes of operations (MOP). These are storing and non-storing mode. Both modes have their pros and cons, and therefore recent developments are more focused on operating the hybrid version of these MOPs. We have contributed a novel hybrid MOP in this paper that uses 2-colorable graph property to decide MOP of devices in an RPL-DODAG. The 2-colorable graph is mapped to two standard MOPs and applied such a way that the parents and child are partition into distinct sets to assign MOP.

Rest of the paper is organized into following sections: A brief discussion on importance of standard MOPs is provided in Sect. 2. The hybrid MOPs techniques reported in the literature so far are reviewed in Sect. 3. The contributed 2-colorable hybrid MOP is presented in Sect. 4. The experiment results and their comparison are analyzed in Sect. 5 followed by concluding points in Sect. 6.

2 Background

RPL supports two standard mode of operations for P2P packet communication among the nodes in a RPL-DODAG. The mode of operation or MOP defines whether a device behave as a router or a non-router nodes for any packet communicated via it. Storing mode indicates that each node in a DODAG stores and maintains a routing table containing routing path to all nodes in its DODAG sub-tree. When the entire network operates on storing mode each packet travels from the source to the Least Common Ancestor (LCA) of the source and destination. The LCA forwards the packets to the destination using its routing table. The DODAG based on storing mode can reduce the routing overhead avoid unnecessary redundant transmissions, however require additional memory for storing each node routing table. For significantly large network, the routing table size increases and becomes overhead for IoT devices.

On the other hand, when all the nodes operate on non-storing mode, they do not maintain routing table for routing packet. When a packet arrives at any device, the device simply directs the packet to its preferred parent until the packet arrives at the sink of the current DODAG. The sink node is considered as a special node which always operates on storing mode. Therefore, the sink is the only node that maintains routing table in non-storing mode and forwards the packet that arrives from a source to its respective destination. The additional memory requirement of non-storing mode is nearly zero, which is suitable for memory constrained IoT Devices. However, each packet needs to travel to reach sink node before it is redirected to the DODAG sub-tree of the destination. Even if the source and destination pair of nodes are present at a lower level DODAG sub-tree, the packet still needs to travels via sink node. This routing process incurs significantly higher communication overhead.

To mitigate the demerits of both the mode, researcher are adapting the hybrid MOP, where a predefined criteria decides whether to operate on storing or non-storing node. As a result, a subset of the IoT devices operate in storing mode, and the rest of the node on non-storing mode. The ratio of storing and non-storing node may vary with the criteria used to decide the storing mode. The hybrid MOP are gaining popularity due to their ability to minimize the communication and/or storage overhead. In the next section, we present the hybrid MOPs that have been designed so far in the literature highlighting their hybrid MOP criteria and characteristics.

3 Related Work

Here, we briefly describe the operational procedure of seven recent hybrid MOPs that utilize mostly the routing metrics such as routing table size, MOP of next child, battery level etc. [8]. Gan *et al.* [2] has proposed a hybrid MOP called Memory-Efficient RPL (MERPL). In MERPL, each device operates on storing mode until the number of routing entries reaches a predefined threshold value. On reaching the threshold value, the node select a non-leaf node in its sub-DODAG having the largest sub-tree to become the storing node. If two non-leaf nodes have the same size, then decision of selection is done on the basis of the smallest identity. The DualMop RPL has been proposed by Ko *et al.* [6]. On receiving a packet for a child node, a parent node first determines the storing mode of its child. The parent node just forward it to the child if child is already using storing mode; otherwise, it generates route, duplicates the source routing header, and finally sends the packet to the child. D-RPL has been proposed by Kiraly *et al.* [5] that addresses the node that failed to declare their DAO by a multicast channel. The root first determines if standard forwarding is feasible for each packet. If such a path cannot be found, the multicast channel is utilized to route the packet to the junction nodes.

The Hop-Interval based Mode Of OPeration Decision (HI-MOPD) scheme has been proposed by Lee *et al.* [7]. In their approach, initially the root computes the hop interval to be maintained between two storing nodes along a path. This is termed as Optimal Hop Interval between Storing Mode (OHIS) value. Then, each intermediate node select their mode by using the OHIS and determines Hop Count after Storing Mode in the second phase (HCS). Each node then compares the OHIS and HCS values. The MOP is non-storing if OHIS is smaller than HCS; otherwise, the node uses storing mode. Adaptive RPL (A-RPL) is proposed by Vyas *et al.* [16]. It is a dynamic mechanism for switching between the MOPs. All nodes initially operate in storing mode. A node removes all entries from the routing table and switches to non-storing mode immediately when its routing table has no more space to add new routes. A method titled hybrid RPL has been proposed by Sukho *et al.* [12]. In this approach, the route data is separated between the storing nodes and the root to reduce the packet transmission overhead at routers. Mishra *et al.* [9] have proposed two variation of hybrid MOPs: the first one is a rank-threshold based MOP decider, whereas the second one is based transmission traffic probability with cellular automata rules.

3.1 Problem Definition

The limited energy resources of a typical IoT device is a concern for adapting non-storing mode, whereas limited memory is an obstacle for opting fully storing mode in a DODAG. A hybrid mode of operation resolves the issues found in storing and non-storing mode. However, it needs to achieve an optimal balance between minimizing transmission and storing overhead. It is observed from the literature that most of the reported techniques try to minimize the storage overhead while compromising the optimization of communication overhead up to a significant level. The recent versions of hybrid MOPs are required to achieve communication overhead nearer to the storing mode while managing the memory requirement up to a lower bound threshold level.

4 Proposed Work

The proposed 2-colorable DAG structured hybrid MOP that not only achieve balance between storing an non-storing node, but also able to reduce the communication overhead for all kinds of P2P communication in RPL.

4.1 The Foundation

A graph $G(V, E)$ is called a 2-colorable graph, if its chromatic number $\chi(G)$ is less than or equal to two. The graphs with no odd cycle are 2-colorable and this is the property that can easily identify whether a graph is 2-colorable. On the other hand, a graph $G(V, E)$ is a bipartite graph, if its vertex set V can be partitioned into two distinct sets A and B in such as way that each edge of G has one of its endpoint in A and other in B. It is obvious that the bipartite graphs are 2-colorable. Whereas, when a 2-colorable graph is not connected, there are more than one way to define the two partition sets A and B. The bipartite graphs represents the models of two distinct types of nodes or entities, where the connectivity are only permitted between two distinct type of objects.

In a hybrid MOP technique for RPL the nodes can be either in storing or non-storing mode in a DODAG depending on the underlying parameters defined by it. Secondly, the techniques proposed in [8] implies that the network performance enhancement is marginal when adjacent node in a DODAG operates in storing mode. In order to achieve a balanced architecture of storing and non-storing nodes for a DODAG, we propose to adapt 2-colorable graph model for deploying hybrid MOP among the nodes of a DODAG. The principles of using 2-colorable or bipartite graph as hybrid MOP is described below.

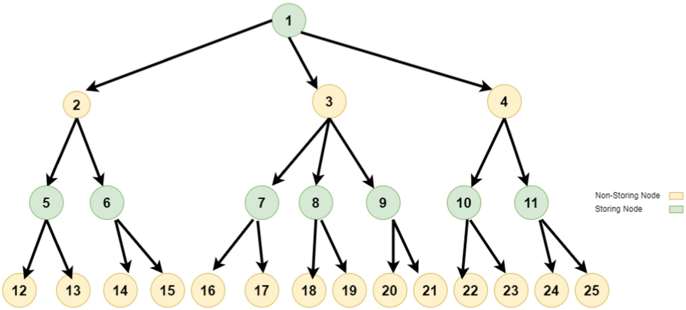


Fig. 1. An Example 2-colorable hybrid MOP in a given DODAG.

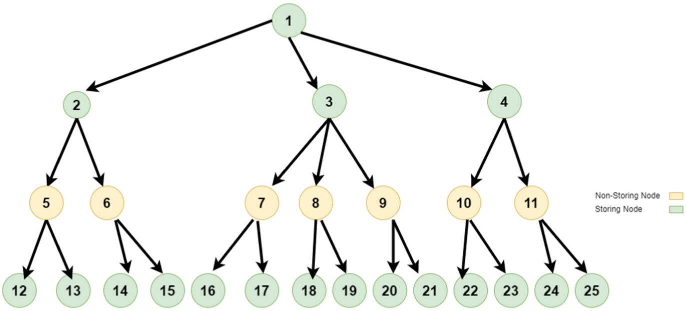


Fig. 2. Switching of mode from Example 1 when the timer expires.

4.2 The Proposed Hybrid MOP Model

To begin with, the sink node of a DODAG is assumed to be always in storing mode and does not belongs to the 2-colorable graph of hybrid MOP. This is because, it is a special node and as per the RPL protocol the sink node has routing entries for each node present in its DODAG. The 2-colorable graph of hybrid MOP is obeyed by each device in such a way that any pair of DODAG parent and child nodes does not share the same MOP at any instance of time. That implies that if a node i has a child j then MOP$(i) \neq$ MOP(j). Initially, MOPs for each node is assigned during the formation of DODAG. The nodes adjacent to the sink are initialized with non-storing mode. The nodes that are present at one-hop away from the sink are and children of adjacent nodes of sink are assigned with storing mode. In this way, nodes of present at every alternate level of DODAG are assigned with same MOP in order to obey the 2-colorable property during the construction of DODAG. An example of an initial DODAG with MOPs is shown in Fig. 1. Here, the yellow colored nodes operate in non-storing mode, whereas green colored nodes operate in storing mode.

Once all the devices are initialized with initial MOPs, a timer is initialized by each device. All the devices in the DODAG are time synchronized in order to start and reset its timer. The duration of the timer is decided based on network data flow statistics and average traffic load at each device. When the timer of a device expires, it switches its current MOP. In other word, when the timer of a node expires, a node currently operating on storing mode switches to non-storing mode and vice versa. Evidently, the DODAG will still maintain the 2-colorable graph property for MOPs. This is because, in a 2-colorable graph the color between the two sets bearing distinct colors can be swapped without violating the 2-colorable properties. Figure 2 shows the switching of MOP from the state of Fig. 1 when the timer expires. According to the proposed hybrid MOP, whenever a timer expires the nodes switches its MOP and reset the timer, and this process continue throughout the lifetime of the DODAG or reconstruction of DODAG whichever is earlier.

4.3 Advantages of Proposed 2-Colorable DODAG Hybrid MOP

The application of 2-colorable graph property for assigning and maintaining the MOP in a DODAG maintains a balanced ratio of the number of storing and non-storing devices in a DODAG. Moreover, since because of 2-colorable property in a DODAG as shown in Figs. 1 and 2, there are storing nodes at every alternating position in each path from a leaf node to the sink. That means, for the P2P communication that involves a pair of source and destination devices (s, d) under the sub-tree of a given node r, the additional amount of transmission incurred by the hybrid MOP is only equal to two. This is because, in the worst-case scenarios the node r operates in non-storing mode, while its parent operates in storing mode according to 2-colorable property. Therefore, the proposed hybrid MOP can achieve a routing performance nearly equal to as of storing mode while incurring a balance storage overhead. In the next section, we experimentally verified the performance of DODAG using the proposed 2-colorable hybrid MOP.

Theorem 1. *The worst case communication overhead of the proposed 2-colorable DODAG hybrid MOP is equal to communication overhead of storing mode plus 2.*

Algorithm 1: The Implementation Procedure of the proposed Hybrid MOP on a node.

```
if DIO received from a parent then
    if the parent's MOP is storing then
        initialize $i$.MOP as non-storing;
    else
        initialize $i$.MOP as storing;
setTimer(MOP_SWITCHING_TIME);
if timer expired then
    if $i$.MOP == storing then
        $i$.MOP = non-storing;
        flush Routing Table of $i$;
    else
        $i$.MOP = storing;
else
    Continue with the current MOP;
```

Proof. In the storing mode, a packet from source node travels until it reach LCA before being redirected to the destination. Let $|P_{i,LCA}|$ denotes the path length from a source i to the LCA of the packet, and $|P_{LCA,dest}|$ denotes the path length from the LCA to destination node in its sub-tree. If we define communication overhead of RPL as the number of transmissions occurred while sending a packet from a source to destination, then the communication overhead of the storing mode per packet is given by $|P_{i,LCA}| + |P_{LCA,dest}|$.

In the proposed 2-colorable hybrid MOP, there may be two possibilities in this case of transmission. First the LCA node of the source and destination pair is currently not operating in the storing mode. However, using 2-colorable property in a DODAG the parent of the LCA is ensured to operate in storing mode. In that case the packet needs to travel to the parent node of LCA and redirected back to LCA for forwarding it to its destination. Therefore, the worst case communication overhead per packet of the proposed 2-colorable hybrid MOP is given by $|P_{i,LCA}|+|P_{LCA,dest}|+2$, which is equal to communication overhead of storing mode plus 2.

Theorem 2. *The number of nodes in the proposed 2-colorable DODAG hybrid MOP that possesses the storage overhead of average number of routing entries per node at any instance of time is either equal to*

$$\frac{(d^2)^{\lfloor \frac{l}{2}\rfloor+2}-1}{(d^2)-1} \;\; or \;\; \frac{(d^2)^{\lfloor \frac{l}{2}\rfloor+1}-1}{(d^2)-1}$$

where l, d are the maximum level of DODAG and average degree of a node respectively.

Proof. If the average degree of a node in DODAG is given by d, that is the average number of nodes that may have the same DODAG parent. In the storing mode, all the nodes including sink operates in storing mode. If we assume that the DODAG has maximum l level of nodes, then the number of nodes operate in storing mode is given by

$$\frac{d^{l+1}-1}{d-1} \tag{1}$$

In the proposed 2-colorable hybrid MOP, only the nodes in the alternate level of the DODAG operates in storing mode at any instance of time. The number of nodes in the odd levels of a DODAG is given by

$$\frac{\left(d^2\right)^{\lfloor \frac{l}{2} \rfloor + 2}-1}{\left(d^2\right)-1} \tag{2}$$

whereas, the nodes in the odd levels of a DODAG is given by

$$\frac{\left(d^2\right)^{\lfloor \frac{l}{2} \rfloor + 1}-1}{\left(d^2\right)-1} \tag{3}$$

Therefore, at any instance of time the number of nodes operating in the storing mode in the proposed 2-colorable hybrid MOP is either equal to Eq. 2 or 3.

5 Results

We have simulated our proposed 2-colorable hybrid MOP in a Python programming environment. We have to compare the performance of our proposed hybrid MOP with APRL, MERPL, HIMOPD, rank-threshold based, and cellular automata (CA) based hybrid MOP by [9]. The network size selected for the experiment is 20 and 50. A timer of five seconds is set in the proposed hybrid MOP for shifting between the two standard modes. A count of 15 pairs of nodes is chosen at random for P2P communications. The metrics used for the evaluation of performance are Transmission count, average path length, and an average number of routing entries per node.

Figure 3 shows the comparison of average transmission count of the proposed 2-colorable hybrid MOP and the standard storing and non-storing MOPs. The transmission count of the proposed hybrid MOP is closer to storing mode, which indicates that the proposed hybrid MOP enables optimal path routing with a marginal higher communication overhead than storing mode. This is possible due to present of storing nodes in every alternate level of DODAG obeying the 2-colorable property of MOP applied on DODAG.

Figure 4 compares the transmission count of proposed hybrid MOP with the existing ones. It is observed that the proposed 2-colorable hybrid MOP has transmission count as the second lowest among all the MOP techniques and it is marginally above the rank-threshold based technique [9]. This count values of the proposed hybrid MOPs clearly shows that using 2-colorable property over

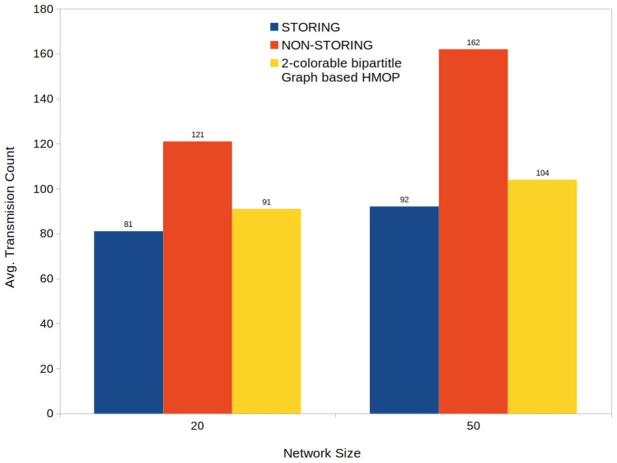


Fig. 3. The comparison of average transmission count with the standard MOPs.

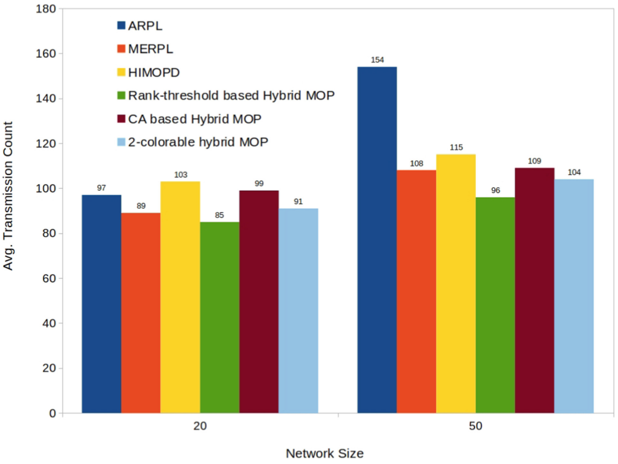


Fig. 4. The comparison of average transmission count with the existing hybrid MOPs.

DODAG, it is still able to achieve optimal routing for all the tested pairs of source and destination. Whereas, the other existing mechanisms incur slightly higher transmission due to lack of storing nodes at the lower levels of the DODAG which gives rise to a longer route to the destination.

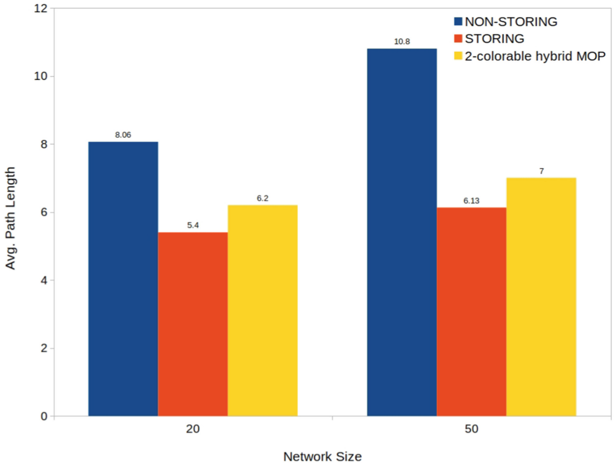


Fig. 5. The comparison of average path length with the standard MOPs.

Figure 5 depicts the comparison of average path length with the standard storing and non-storing modes. The non-storing mode possesses higher path length due to establishing all communication paths via sink node. The proposed hybrid MOP is marginally higher than the storing nodes due to comparatively lesser number of storing nodes presents in the DODAG. This is an optimal result of proposed MOP that achieves path length closes to standard storing MOP with lesser number of nodes operating in the storing mode compared to it.

When the average path length of proposed 2-colorable hybrid MOP is compared with existing hybrid MOPs as shown in Fig. 6, it is observed that the proposed hybrid MOP have second shortest average path length. This is due to presence of storing nodes at each alternate level of DODAG that minimizes the path travelled by a packet to reach its destination node.

The comparison of average number of routing entry per node with standard and existing hybrid MOP is shown inf Figs. 7 and 8 respectively. The number of routing entry in a routing table of a node is zero if a node is operating on non-storing mode and is equal to number of active children nodes in its DODAG sub-tree while a node uses storing mode. It is observed that the average routing entry per node of 2-colorable hybrid MOP lies between storing and non-storing and measured to be slightly higher compared to existing scheme for the network size of 50. This is because, the number of children in a DODAG sub-tree increases with its network size. The methods such as HIMOPD, ARPL, rank-threshold based hybrid MOPs use other heuristics to determine MOP of a device. As a result, the number of storing nodes in the DODAG are lesser than the proposed one and this leads to fewer entries in the routing table.

From all the results presented above, we inferred that the proposed 2-colorable hybrid MOP achieve well-balanced DODAG network of nodes operating in storing and non-storing nodes using 2-colorable property over DODAG.

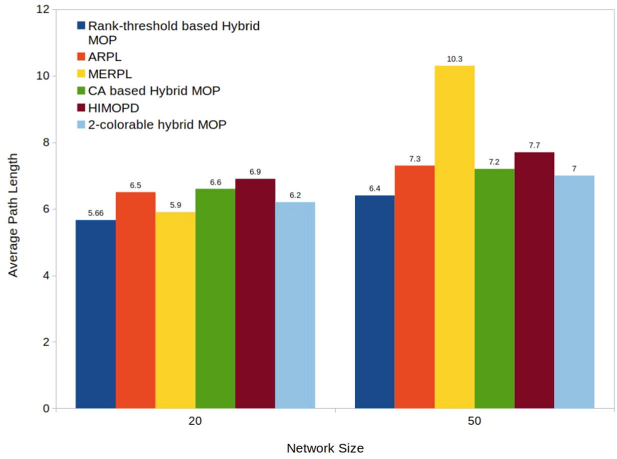


Fig. 6. The comparison of average path length with the existing MOPs.

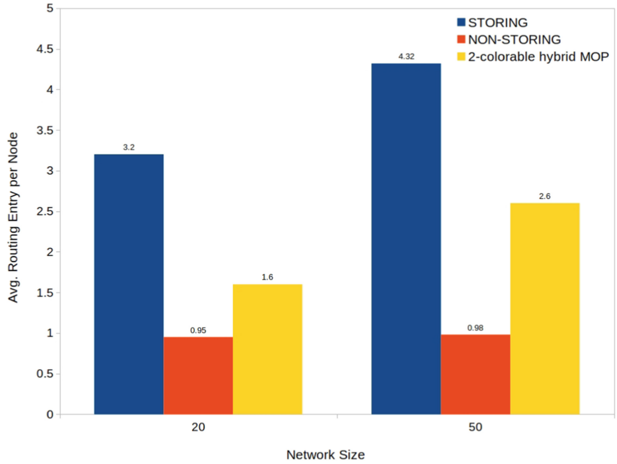


Fig. 7. The comparison of average routing entry per node with the standard MOPs.

As a consequence, it reduces the communication overhead required for any P2P communications in the network. The average path length indicates that the routing overhead of the proposed hybrid MOP is quite lesser than the existing MOPs such as ARPL, MERPL, HIMOPD, and CA based hybrid MOPs. However, due to this balanced ratio of nodes, the proposed MOP possesses a slighter higher storage overhead for higher network size.

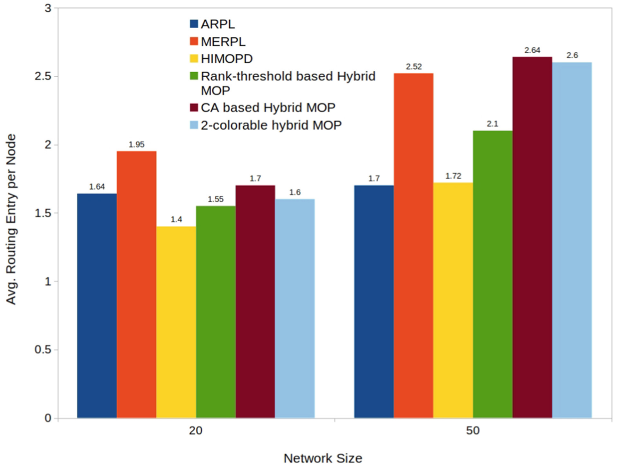


Fig. 8. The comparison of average routing entry per node with the existing MOPs.

6 Conclusion and Future Work

In this research article, we introduce a novel technique for achieving a hybrid MOP in the RPL. Our approach is based on a 2-colorable graph architecture, leveraging the bipartite graph property to determine the MOP of each node in the DODAG-based RPL protocol. We impose the condition that parent and child nodes cannot share the same mode (color), ensuring a balanced distribution of nodes operating in the two standard MOPs. Experimental results demonstrate that our proposed hybrid MOPs effectively reduce communication overhead and yield smaller average path lengths for P2P communications in RPL.

Furthermore, our work can be extended to incorporate other existing logistics used in hybrid MOPs, such as rank-based, ARPL, HIMOPD, to create a more sophisticated hybrid MOP that further improves the achieved results. This opens avenues for future research and optimization in the field of hybrid MOP techniques in RPL-based networks.

Acknowledgment. The statements made herein are solely the responsibility of the authors. This publication is based upon work supported by Khalifa University under Award No. FSU-2022-018.

References

1. Brandt, A., et al.: RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks. RFC 6550, March 2012. https://tools.ietf.org/html/rfc6550
2. Gan, W., Shi, Z., Zhang, C., Sun, L., Ionescu, D.: MERPL: a more memory-efficient storing mode in RPL. In: 2013 19th IEEE International Conference on Networks (ICON), pp. 1–5. IEEE, Singapore (2013). https://doi.org/10.1109/ICON.2013.6781985

3. Imteaj, A., Thakker, U., Wang, S., Li, J., Amini, M.H.: A survey on federated learning for resource-constrained IoT devices. IEEE Internet Things J. **9**(1), 1–24 (2022). https://doi.org/10.1109/JIOT.2021.3095077
4. Kalita, A., Khatua, M.: 6TiSCH-IPv6 enabled open stack IoT network formation: a review. ACM Trans. Internet Things **3**(3), 1–36 (2022)
5. Kiraly, C., Istomin, T., Iova, O., Picco, G.P.: D-RPL: overcoming memory limitations in RPL point-to-multipoint routing. In: 2015 IEEE 40th Conference on Local Computer Networks (LCN), pp. 157–160. IEEE, Clearwater Beach, FL, USA (2015). https://doi.org/10.1109/LCN.2015.7366295
6. Ko, J., Jeong, J., Park, J., Jun, J.A., Gnawali, O., Paek, J.: DualMOP-RPL: supporting multiple modes of downward routing in a single RPL network. ACM Trans. Sens. Netw. **11**(2), 39:1–39:20 (2015). https://doi.org/10.1145/2700261
7. Lee, S., Jeong, Y., Moon, E., Kim, D.: An efficient MOP decision method using hop interval for RPL-based underwater sensor networks. Wireless Pers. Commun. **93**(4), 1027–1041 (2017). https://doi.org/10.1007/s11277-017-3964-2
8. Mishra, A.K., Singh, O., Kumar, A., Puthal, D.: Hybrid mode of operations for RPL in IoT: a systematic survey. IEEE Trans. Netw. Serv. Manage. **19**(3), 3574–3586 (2022). https://doi.org/10.1109/TNSM.2022.3159241
9. Mishra, A.K., Singh, O., Kumar, A., Puthal, D., Sharma, P.K., Pradhan, B.: Hybrid mode of operation schemes for P2P communication to analyze end-point individual behaviour in IoT. ACM Trans. Sens. Netw. **19**(2), 1–23 (2022)
10. Mishra, P., Puthal, D., Tiwary, M., Mohanty, S.P.: Software defined IoT systems: properties, state of the art, and future research. IEEE Wirel. Commun. **26**(6), 64–71 (2019)
11. Mishra, S.K., Puthal, D., Sahoo, B., Sharma, S., Xue, Z., Zomaya, A.Y.: Energy-efficient deployment of edge dataenters for mobile clouds in sustainable IoT. IEEE Access **6**, 56587–56597 (2018)
12. Oh, S., Hwang, D., Kim, K., Kim, K.H.: A hybrid mode to enhance the downward route performance in routing protocol for low power and lossy networks. Int. J. Distrib. Sens. Netw. **14**, 155014771877253 (2018). https://doi.org/10.1177/1550147718772533
13. Sahoo, B., Rath, S., Puthal, D.: Energy efficient protocols for wireless sensor networks: a survey and approach. Int. J. Comput. Appl. **44**(18), 43–48 (2012)
14. Vasseur, J., Kim, M., Pister, K., Dejean, N., Barthel, D.: Routing Metrics Used for Path Calculation in Low-Power and Lossy Networks. RFC 6551, March 2012. https://tools.ietf.org/html/rfc6551
15. Vilajosana, X., Watteyne, T., Chang, T., Vučinić, M., Duquennoy, S., Thubert, P.: IETF 6TiSCH: a tutorial. IEEE Commun. Surv. Tutorials **22**(1), 595–615 (2020). https://doi.org/10.1109/COMST.2019.2939407
16. Vyas, K., Sengupta, J., Bit, S.D.: ARPL: supporting adaptive mixing of RPL modes to overcome memory overflow. In: 2018 IEEE International Symposium on Smart Electronic Systems (iSES) (Formerly iNiS), pp. 124–129. IEEE, Hyderabad, India (2018). https://doi.org/10.1109/iSES.2018.00035

Security by Design for IoT (SbD)

Role-Based Access Control in Private Blockchain for IoT Integrated Smart Contract

Darwish Al Neyadi(✉), Deepak Puthal, Joy Dutta, and Ernesto Damiani

Department of EECS, Khalifa University, Abu Dhabi, UAE
{100061316,deepak.puthal,joy.dutta,ernesto.damiani}@ku.ac.ae

Abstract. Role-based access control (RBAC) is a mechanism that controls access to resources within an organization based on the roles of individual users. This RBAC can be used in the context of an IoT-integrated smart contract for a private blockchain to govern access to smart contract functions and data based on the responsibilities of the system's participants. By preventing unauthorized access to vital functions and data, RBAC can help assure the security and integrity of an IoT-integrated smart contract. In this study, we investigate novel methods to devise a smart contract process that enables data sharing among stakeholders for IoT-based applications to provide complete access control implementation in a private blockchain environment. Here, we have developed and verified our proposed access control mechanism with an added layer of machine learning-based security for an Ethereum-based private blockchain to securely handle IoT-based application data.

Keywords: Blockchain · Smart contracts · dApp · Ethereum · Access Control · Machine Learning · IoT

1 Introduction

In recent years, blockchain technology has revolutionized various industries, providing a decentralized, secure, and transparent framework for data management. It can provide a powerful and versatile infrastructure for IoT-based applications, helping to ensure the security, reliability, and efficiency of data transmission and processing [11]. For real-life IoT-based application implementation, private blockchains are generally preferred over public blockchains due to their greater security, scalability, cost-effectiveness, customization, and regulatory compliance [12]. On the other hand, Role-based access control (RBAC) is effective from a security perspective because it follows the principle of least privilege, provides granular access control, simplifies administration, provides auditing capabilities, and helps organizations meet compliance requirements [5]. By implementing RBAC, organizations can improve their security posture and reduce the risk of unauthorized access to critical functions and data.

Published by Springer Nature Switzerland AG 2024
D. Puthal et al. (Eds.): IFIPIoT 2023, IFIP AICT 684, pp. 227–245, 2024.
https://doi.org/10.1007/978-3-031-45882-8_16

Thus, if the proven RBAC mechanism is utilized for handling access control in a private blockchain, it could pave new ways for widespread IoT applications to be secure and trustworthy [7]. Integrating RBAC with a private blockchain requires careful consideration of the security, governance, and privacy implications of the RBAC model. It is important to have a well-designed RBAC policy and to ensure that it is enforced and audited effectively to maintain the security and integrity of the blockchain network [4]. This research aims to address these challenges by designing a resilient system combining private blockchain technology's benefits with the RBAC model. Furthermore, the research investigates the development of a smart contract process that facilitates secure data sharing among different stakeholders, complete with access control implementation, ultimately paving the way for a more efficient and secure IoT ecosystem.

The rest of the paper is organized as follows: Sect. 2 discusses related work in this field and identifies the scope of work. Next, our proposed solution approach is discussed in Sect. 3. The effectiveness of the solution is discussed in Sect. 4 and finally, the work is concluded in Sect. 5 with future directions.

2 Background Study

Access control is an important mechanism for ensuring secure and controlled access to data and resources in computer systems [3]. In recent years, the application of RBAC in blockchain systems has received increasing attention. This section provides a brief overview of some of the existing literature on access control in private blockchain systems.

A study explored the use of blockchain for access control in untrusted cloud storage [13]. The researchers developed an access control system employing a ciphertext-policy with dynamic attributes, utilizing a blockchain ledger to record immutable security events, such as key generation, access policy assignment, and access requests. Privacy of secret keys is ensured through a set of cryptographic systems, with only hash codes representing ciphertexts being transferred through the block-chain. This system was implemented using Ethereum and its smart contract capabilities. Also, preserving privacy is a critical consideration in distributed systems. One research paper addressed this issue within the context of a personal health record system [15]. This system allows patients to store, manage, and share their data with specific individuals while leveraging blockchain based access control for tamper resistance and privacy preservation. Next, in [16], authors present a dynamic and lightweight attribute-based access control system. They build a DApp-based access control framework to adapt to IoT device boundaries and keep tamper proof quickly. To combat security fluctuations induced by IoT devices' susceptibility, a Markov chain-based trust management strategy is presented. To test the concept, the authors created a system prototype on Ethereum, which suggests the proposed approach offers secure, high-throughput, and adaptable IoT access control.

Another recent article, [8], employs an RBAC strategy with a blockchain-enabled smart contract to govern permissions for organizational user roles.

Using the Ethereum blockchain framework and its smart contract competencies, the proposed approach models user-resource interactions. Alternatively, another study proposed a mechanism which delivers confidentiality-based authentication by employing a hashing algorithm and a pass that cannot be distinguished from its proprietor [1,9]. On an Ethereum-based prototype network configuration, where smart contracts enable negotiations regarding a trustless interaction, this was demonstrated. In this context, another research article [10] identifies that conventional RBAC schemes are centrally managed, and the distribution of a user's role is missing fine granularity. It also identifies the distribution of responsibility and authorization is fixed, which is not compatible with the distributed and dynamic network structures of today. Consequently, they introduce a dynamic and fine-grained RBAC model, DF-RBAC, which is capable of the flexible allotment of responsibilities by resource owners and the verification of selected roles' security.

The studies reviewed in this section demonstrate that RBAC is effective in controlling access to sensitive data and resources in blockchain systems. This also revealed a significant gap in defining role-based access control for blockchain systems. Existing solutions are either fully centralized using private blockchains or entirely blockchain-based, resulting in slow interaction times. To bridge this gap, the proposed approach introduces four distinct user groups, each with unique attributes, allowing for efficient and swift verification and data upload while maintaining the security and integrity of the blockchain. This structure preserves tailored access for individual users, with authentication and authorization closely monitored throughout the process to ensure a secure and seamless user experience. In the next section, we will discuss our proposed methodology in detail [1].

3 Proposed Methodology

In our proposed methodology, users interact with a front-end interface to input data and request specific actions, such as data storage, retrieval, or transaction processing. This user-facing interface communicates with a server responsible for verifying user identity and encrypting sensitive information. To achieve this, the server employs advanced cryptographic techniques and digital signatures, ensuring secure and tamper-proof data transmission. Once verified and encrypted [14], the server communicates with a back-end system that leverages Web 3.0 technology to submit transactions and interact with Ethereum blockchain. Multiple smart contracts are deployed on the Ethereum network, each with specific access control functions, data hash storage capabilities, and token-based authorization mechanisms. These contracts facilitate secure, decentralized data management and enable seamless interaction between users and the blockchain. IoT devices, however, bypass the front-end interface and directly interact with the server's verification and encryption system. This streamlined process allows IoT devices to securely and efficiently communicate with the server, ensuring seamless integration into the larger ecosystem. The design description of the proposed system

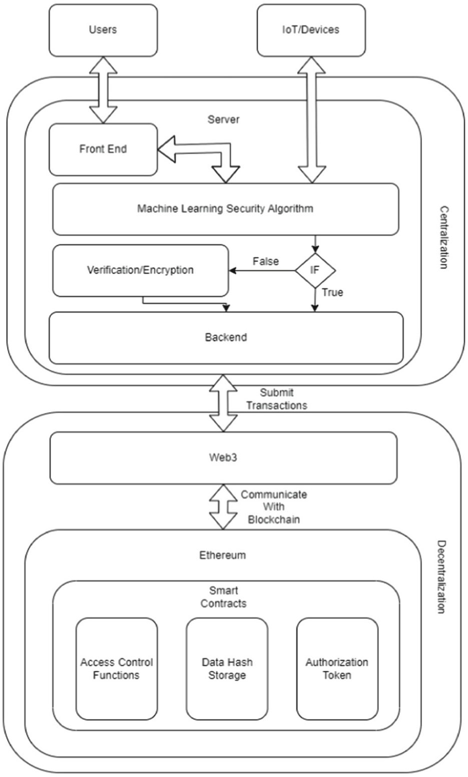


Fig. 1. Proposed Methodology

is shown in Fig. 1. To understand the workings of the system, we will further discuss the major steps in detail next.

3.1 Semi-Decentralized Authentication

Authentication is the first step involved in the thorough process of access control in private blockchains. Without successful authentication, users or IoT devices are not allowed to interact with the blockchain. The process of securely authenticating a user/IoT device and verifying their digital identity involves several steps, including verifying signatures, digital certificates, tokens, IP addresses, and MAC addresses. This multi-step process helps ensure the authenticity and integrity of the user's credentials and their connection to the Dapp. Now we will discuss the steps involved in authentication in detail.

First, the user needs to be authenticated. This involves providing a digital signature using *MetaMask*. Next, the user's signature is verified using the *ethers.js* library, a popular JavaScript library for interacting with the Ethereum blockchain. This *ethers.js* helps in validating the digital signature associated

Algorithm 1. Server Algorithm

```
procedure User Group
   Define an Auth class with methods signMessage and verifyCertificate.
    function signMessage
        Extract the walletAddress from the request body
        Check if the walletAddress exists
        Retrieve the user associated with the walletAddress using the UserService
        if user is found then
            Send a response with the FRONTEND_MESSAGE_TO_SIGN
        else
            Store the IP and MAC addresses, and generate a certificate
            Get the user's IP address using getUserIpAddress
            Get the user's MAC address using getMacAddress
            Generate a certificate using generateCertificate
            Send a response containing the FRONTEND_MESSAGE_TO_SIGN and the generated certificate
        end if
    end function
    function verifyCertificate
        Extract walletAddress from the request body
        Extract the certificate and privateKey from the request headers
        Verify the certificate using verifyCertificate
        Send a response with the verification result
    end function
end procedure
```

with the user's public key, ensuring that the data has not been tampered with and that it originates from the genuine user.

Following the signature verification, the digital certificate is verified using certificate encryption and the user's private key. The certificate's authenticity is checked by decrypting the digital signature. If the decrypted signature matches the certificate's content, it confirms that the certificate is genuine. This step ensures that the user's public key and identifying information are accurate and trustworthy. Subsequently, the system verifies tokens through a smart contract and the *ethers.js* library. This involves checking the user's tokens, which may represent their digital assets or authorization to perform specific actions within the blockchain-based application. By interacting with the smart contract, the system confirms that the user has the appropriate tokens and permissions.

Lastly, the system verifies the user's IP address and MAC address. The IP address is a numerical label assigned to devices connected to a network and helps identify the user's location. The MAC address is a unique identifier assigned to a network interface controller (NIC) for communication within a network. By verifying both the IP and MAC addresses, the system ensures that the user's device is authentic and hasn't been compromised or spoofed. The detailed procedure for the same is shown in Algorithm 1. This whole comprehensive process helps maintain the security and integrity of online services and platforms, protecting users and their data from unauthorized access or tampering.

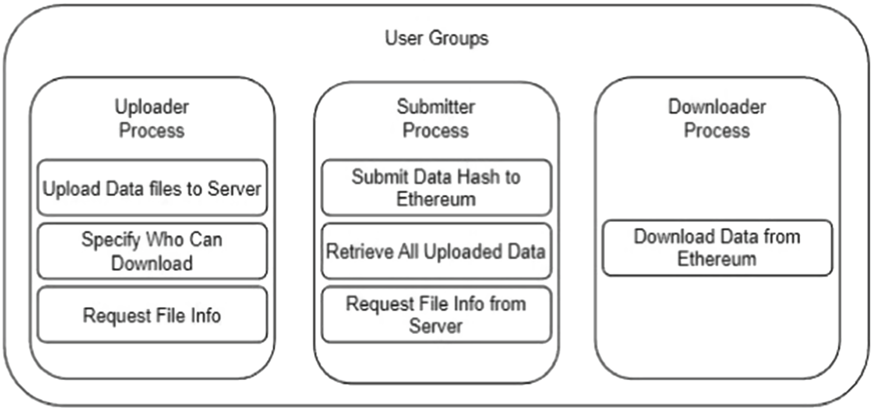

User Groups
Uploader Process
Upload Data files to Server
Specify Who Can Download
Request File Info
Submitter Process
Submit Data Hash to Ethereum
Retrieve All Uploaded Data
Request File Info from Server
Downloader Process
Download Data from Ethereum

Fig. 2. User Group Processes

3.2 Decentralized User Groups Interaction Processes

We have grouped user processes as Uploader Process, Downloader Process and Submitter Process. Different processes have different roles in our proposed system design. These processes are playing a key role in implementing RBAC on a private blockchain by utilizing Smart Contract. We will discuss these three individual processes one by one (Fig. 2).

Uploader Process: The uploader process begins with user authentication, which involves verifying the user's private keys, digital signature, digital certificate, tokens, IP address, and MAC address. This comprehensive authentication ensures that the user is genuine and authorized to access the system. Once the user is authenticated, they can proceed to upload files to the database server.

After uploading the files, the user can view or download the uploaded files from the blockchain using the InterPlanetary File System (IPFS) and encryption. IPFS is a peer-to-peer file-sharing protocol that allows for efficient and decentralized storage and retrieval of files. Encryption ensures that only authorized users can access the files, providing an additional layer of security. Details of the Uploader Process are further detailed in the Algorithm 2.

The Uploader Process Algorithm involves creating an Uploader class with three distinct methods: uploadFile, getUploadedData, and downloadFile. Each of these methods corresponds to a specific function in the data uploading process.

The uploadFile function begins by checking if the request contains a file. If a file is present, the data is encrypted for security purposes. The encrypted content is then uploaded to the InterPlanetary File System (IPFS), a protocol and network designed to create a content-addressable, peer-to-peer method of storing and sharing hypermedia in a distributed file system. Following the upload, a new 'Files' object is created with the necessary properties and saved to the database. A response is then sent containing the newFile object. However, if the request

Algorithm 2. Uploader Process

```
procedure Uploader Process
  Create an Uploader class with methods: uploadFile, getUploadedData, and downloadFile.
    function uploadFile
        if request contains a file then
            Encrypt the file data
            Upload the encrypted content to IPFS
            Create a new Files object with necessary properties
            Save the new Files object to the database
            Send a response containing the newFile object
        else
            Throw a BadRequest error
        end if
    end function
    function getUploadedData
        Extract walletAddress and other filters from the request
        Create an object with uploaderAddress and other optional filters
        Call fileService.getFile with the created object
        Send a response with the retrieved file data
    end function
    function downloadFile
        Extract ipfsHash from the request parameters
        Find the file in the database using the ipfsHash
        if file is found then
            Fetch the file data from IPFS
            Decrypt the file data
            Create a temporary folder if it doesn't exist
            Define a temporary file location for the downloaded file
            Write the decrypted data to the temporary file location
            Start the file download, passing the temporary file location and the original filename
            After successful download, remove the temporary file
        else
            Throw a BadRequest error
        end if
    end function
end procedure
```

does not contain a file, a BadRequest error is thrown, indicating that the user's request was not properly formed.

Next is the getUploadedData function, which is used to retrieve the uploaded data. The function extracts the walletAddress and any other filters from the request, and an object is created with uploaderAddress and other optional filters. The function then calls fileService.getFile with the newly created object, and a response is sent with the retrieved file data.

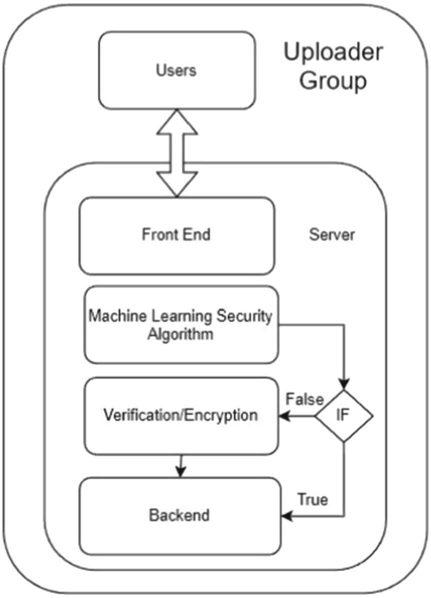


Fig. 3. Uploader Methodology Interaction

The third function is downloadFile, which is used to download the previously uploaded file. It begins by extracting the ipfsHash from the request parameters, which is a unique identifier for the file in the IPFS. It then checks the database for the file using the ipfsHash. If the file is found, the function fetches the file data from IPFS and decrypts it. The decrypted data is then written to a temporary file location that is created if it doesn't already exist. The function initiates the file download, passing the temporary file location and the original filename. After the successful download, the temporary file is removed. However, if the file is not found in the database, a BadRequest error is thrown.

The Uploader Process Algorithm concludes at this stage, having completed the upload, retrieval, and download of the file (Fig. 3).

Downloader Process: This process begins with authenticating the user to ensure they have the necessary permissions to access and download files. Several authentication mechanisms are employed, including private keys, digital signatures, digital certificates, tokens, and the verification of the user's IP and MAC addresses. These mechanisms work together to create a secure and robust authentication process, ensuring that only authorized users can access the files.

Once the user has been successfully authenticated, they can proceed to access the downloadable files. These files are typically organized and displayed in a user-friendly interface, allowing users to browse and select the files they wish to download. In some cases, additional information about the files, such as descriptions or previews, may be available to help users make informed decisions about the files they want to download. Upon selecting the desired files, the user is prompted to complete a transaction using *MetaMask*. It is integrated into the user's browser, enabling them to review the transaction details and confirm the transaction. This process may involve paying for the files or accepting any terms and conditions associated with the files' usage.

Finally, once the transaction has been successfully completed, the user can proceed to download the files. The files are typically compressed and transferred securely to the user's device, ensuring that the download process is efficient and safe. Upon completion, the user can decompress the files and access them on their device, ready for use as needed.

Submitter Process: Similar to the uploader process, the submitter process starts with user authentication. The system verifies the user's private keys, digital signature, digital certificate, tokens, IP address, and MAC address to confirm their identity and authorization.

Once authenticated, the user can submit the previously uploaded files from the database to the blockchain. This process involves registering the files' metadata and associated transactions on the blockchain, providing transparency, immutability, and security for the records. After submitting the files, the user completes the transaction using *MetaMask*, a popular browser-based wallet for interacting with the Ethereum blockchain. *MetaMask* allows users to manage their digital assets, sign transactions, and interact with decentralized applications (dApps) securely. Finally, the submitter user can view all the submitted files on the blockchain. This allows them to keep track of their submissions and access the history of transactions, ensuring the integrity and transparency of the records. For more insight into how the submitter process works, refer to Algorithm 3, where further details of the process can be found.

The Submitter Process Algorithm involves the creation of a Submitter class with five distinct methods: getSubmittedData, getSubmittedDataDB, getAllUploadedData, submitData, and fileDetails. Each method serves a specific purpose in handling submitted data. The getSubmittedData function begins by calling the dataStore.getSubmittersAllData function with a specific walletAddress as a parameter. The resulting response is then mapped to a new array of objects, and a response with this mapped data array is sent.

Next, the getSubmittedDataDB function comes into play. It starts by extracting the walletAddress from the request body. The function then calls fileService.getFile with submitterAddress and a status indicating "SUBMITTED". Finally, a response is sent containing the data retrieved. The getAllUploadedData function is used to retrieve all the data that has been uploaded. It calls the fileService.getFile function with a status indicating "UPLOADED". The data retrieved is then sent as a response.

The submitData function is responsible for the data submission process. It starts by extracting relevant data from the request body. It then calls fileService.getFile with ipfsHash and a status indicating "UPLOADED". A new object is created containing submitterAddress, a status of "SUBMITTED", and other

Algorithm 3. Submitter Process

```
procedure Submitter Process
    Create a Submitter class with methods: getSubmittedData, getSubmittedDataDB, getAllUploadedData, submitData, and fileDetails.
    function getSubmittedData
        Call dataStore.getSubmittersAllData with walletAddress
        Map the response to a new array of objects
        Send a response with the mapped data array
    end function
    function getSubmittedDataDB
        Extract the walletAddress from the request body
        Call fileService.getFile with submitterAddress and status "SUBMITTED"
        Send a response with the retrieved data
    end function
    function getAllUploadedData
        Call fileService.getFile with status "UPLOADED"
        Send a response with the retrieved data
    end function
    function submitData
        Extract relevant data from the request body
        Call fileService.getFile with ipfsHash and status "UPLOADED"
        Create an object with submitterAddress, status "SUBMITTED", and other properties
        Call fileService.updateFile with id and the created object
        Send a response with the update result
    end function
    function fileDetails
        Extract ipfsHash from the request body
        Call fileService.getFileByipfs with ipfsHash
        Send a response with the file details
    end function
end procedure
```

necessary properties. The function then calls fileService.updateFile with an id and the newly created object. A response is sent with the update result.

The final function, fileDetails, is used to retrieve the details of a specific file. It begins by extracting the ipfsHash from the request body. It then calls fileService.getFileByipfs with ipfsHash. The details of the file are then sent as a response. The Submitter Process Algorithm concludes after this stage, having effectively handled the retrieval, update, and submission of data (Fig. 4).

In conclusion, the uploader and submitter Processes involve several steps to ensure the secure and efficient handling of files on the blockchain. Both processes begin with thorough user authentication, followed by uploading and submitting files to the database server and the blockchain, respectively. Along with these, the downloader process's seamless integration of authentication, file access, transaction management, and secure file transfer provides an effective and user-friendly

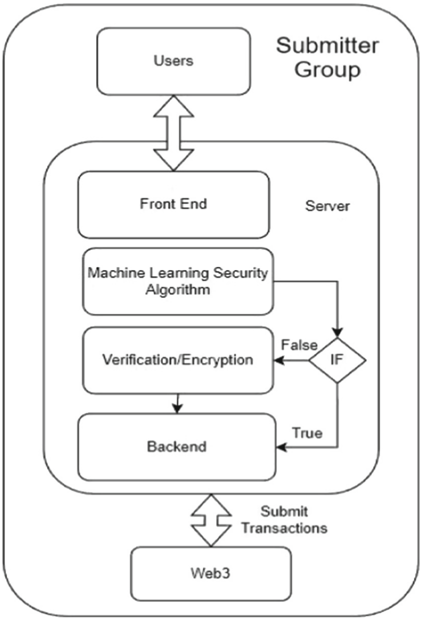


Fig. 4. Submitter Methodology Interaction

experience for downloading files. The use of IPFS and encryption, along with tools like *MetaMask*, allows users to securely manage and interact with their data on the blockchain.

3.3 Role of Smart Contract

Smart Contracts provide a powerful mechanism for enforcing Role-Based Access Control in private blockchains. They provide transparency, automation, and flexibility in managing access control policies, making them an essential component of any secure and robust blockchain system. In a private blockchain, smart contracts can be used to enforce RBAC by defining the roles and permissions for each user. These roles can be used to restrict access to certain functionalities or data within the system. The smart contract can be designed in such a way that only users with the appropriate roles can perform certain actions or access specific data. We will now discuss the algorithm's functionality in detail.

We have used designed our smart contracts in Solidity for the Ethereum blockchain. Here, in this research the *OpenZeppelin* Contracts v4.4.1 library is used for realizing the *Ownable* contract pattern in Solidity. The Ownable contract provides a basic access control mechanism, in which an owner account has exclusive access to specific functions. By default, the owner's account is the one that deploys the contract, but this can be changed later using the *transferOwnership* function. The owner function is a public view function that returns the address of the current owner. The *onlyOwner* modifier is provided to restrict function calls to the current owner. If the caller is not the owner, an error message is thrown. The *renounceOwnership* function allows the current owner to relinquish ownership of the contract, effectively disabling any functionality that is exclusive to the owner. Lastly, the *transferOwnership* function is an internal function that handles the actual transfer of ownership. It updates the owner variable and emits the *OwnershipTransferred* event.

A Solidity smart contract named *DataStore* was created to utilize the *Open−Zeppelin* library. The contract manages data uploads and submissions, tracks the roles of users (uploader, submitter, and admin), and handles minting tokens based on role and actions. The contract stores information about uploaded data in the *HashInfostruct* and maintains several arrays and mappings to track data, user roles, and minted tokens. It also emits various events to capture the addition and removal of users from roles, as well as data added and removed. The contract has several role-based modifiers to restrict access to specific functions based on the user's role. Also, functions for adding and removing users in different roles are provided in our design. These functions enforce the necessary access control, update the relevant mappings and arrays, mint tokens for the users, and emit the corresponding events. We have designed several *getter* functions to retrieve data from the contract based on user roles and data indexes. Our defined *getMintedTokens* function returns the total number of minted tokens for a user based on their role as an *uploader* or *submitter*. Finally, the internal function *_authorize − Upgrade* is required to authorize the upgrades to the contract implementation.

Thus here, the use of smart contracts provides several benefits in enforcing RBAC in private blockchains. First, smart contracts provide a tamper-resistant and transparent mechanism for enforcing access control policies. All transactions on the blockchain are recorded and cannot be altered, which ensures that access control policies are enforced consistently and fairly. It also provides automation and efficiency in enforcing access control policies. Once the access control policies are defined in the smart contract, the system can automatically enforce them without requiring manual intervention from the system administrator. Along with these, it provides flexibility in managing RBAC. The system administrator can easily update or modify the access control policies by updating the smart contract. This allows for easy adaptation to changing business requirements or security threats.

3.4 Role of Machine Learning

Integrating Machine Learning (ML) into cybersecurity methodologies has induced a significant paradigm shift, ushering in a proactive strategy for security and threat identification. Here, the ML layer adds one more layer of security to the overall design of the system. By setup, our system collects some vital information that can be used to detect user authenticity. For this purpose, a comprehensive dataset, sourced from reference [2], consisted of 10,000 unique data points, each representing different patterns and decisions encompassing diverse user-related information was assembled, including device specifications, IP addresses, geographical coordinates (latitude and longitude), unique visitor IDs, and information about browsers and operating systems used. This information is vital in identifying unique usage patterns, potential anomalies, and risk factors related to each user interaction. After data collection, it underwent preprocessing to ensure its suitability for the model, with most of the data synthesized for a larger dataset. Missing values were imputed, outliers were managed, and categorical variables were correctly encoded. This stage is critical as the quality of data directly impacts the model's learning ability and, consequently, its prediction accuracy.

With the data preprocessed, the different supervised ML models were trained, enabling them to learn intricate patterns and relationships within the data, recognize normal user behavior, and discern the subtleties that distinguish a legitimate user from a potentially harmful one. Due to the supervised nature of the problem at hand, which necessitates labeled data for intruder prediction, we have experimented extensively with various supervised machine learning models to determine which one is the best fit for our IoT application scenario. Here, we have shown comparison of logistic regression (LR), Naive Bayes (NB), Decision Tree (DT), and Random Forest (RF) models for selecting the most appropriate one for our problem scenario. Upon training, different model's predictive capabilities were checked. Out of these models, the RF model outperformed other models, which we will discuss further in the result section.

Thus, incorporating the supervised ML model improves the system's security while improving the user experience. Legitimate users encounter fewer disruptions, and potential threats are more readily identified and addressed. It's important to note that the model continues to learn and adapt over time with new data, enabling it to identify and respond to emerging threat patterns and maintain the strength of the security framework. Integrating the Random Forest model into the security protocol has significantly heightened the system's predictive and management capabilities regarding potential threats. By continually learning from the data, it provides a dynamic, intelligent security solution that safeguards the system and its users.

4 Results and Discussions

With our Solidity-based testbed implementation, we have calculated the overall time taken by general authentication, uploading authentication, and submitting transactions, along with fine-grained details. We have also tested the system for separate user groups to verify if the end user is able to interact with this secure data management system efficiently without compromising speed. We will discuss our findings now.

The results presented in Table 1 demonstrate the various stages and timings involved in verifying an Ethereum wallet and authenticating it with the proposed methodology. The general authentication process, which includes verifying the digital certificate, token, wallet, IP address, and MAC address, takes a total of

1 min and 37 s (m:ss). The certificate verification is relatively quick, taking only 6.149 milliseconds (ms), while the token verification is slightly longer at 1 min and 27 s. Wallet verification and IP address verification are both extremely fast, with timings of 2.454 ms and 0.115 ms, respectively. MAC address verification, however, takes a significant amount of time, around 10.017 s. The details of the Ethereum block processing are shown in Fig. 5a.

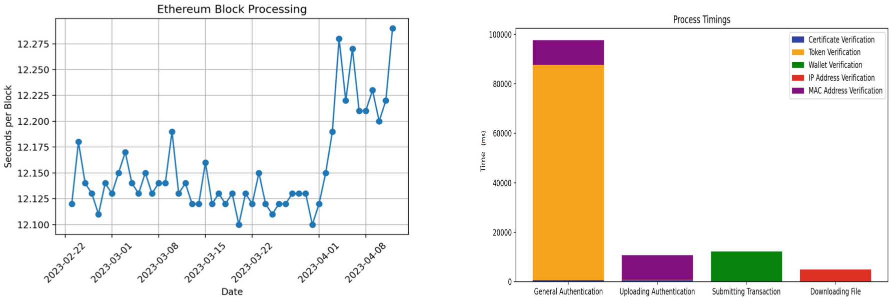
Table 1. Process Timing Results

Processes	Durations
General Authentication	1:37 (m:ss)
Certificate Verification	6.149 ms
Token Verification	1:27 (m:ss)
Wallet Verification	2.454 ms
IP Address Verification	0.115 ms
MAC Address Verification	10.017 s
Uploading Authentication	10.095 ms
Certificate Verification	7.993 ms
Token Verification	53.692 ms
Wallet Verification	3.603 ms
IP Address Verification	0.083 ms
MAC Address Verification	10.031 s
Submitting Transaction	12.2 s
Downloading File	5 s

When it comes to uploading authentication, the process is generally quicker. Certificate verification takes 7.993 ms, token verification takes 53.692 ms, wallet verification takes 3.603 ms, IP address verification takes 0.083 ms, and MAC address verification takes 10.031 s. Overall, the uploading authentication process is faster compared to the general authentication process.

Next, the process of submitting a transaction takes 12.2 s, and downloading a file requires 5 s. These results provide insight into the time efficiency of each component of the Ethereum wallet verification and authentication process. Allowing for separate user groups makes the end user able to interact with this secure data management system at the same speed it would usually take to interact with any centralized system, however in the backend, they gain the benefit of the blockchain without waiting for confirmation time. The process timings, split by type of verification, are shown in Fig. 5b.

Then, for the added layer of security, different supervised ML models have been explored here that exhibit diverse levels of prediction accuracy, as shown in Fig. 6. Here, accuracy signifies the proportion of accurate predictions out of total predictions using a 10 Fold Cross Validation method. The Random Forest



(a) Ethereum Block Processing

(b) Process timings split by type of verification

Fig. 5. General Process timing split

model continues to lead with a mean accuracy of 96%, and a superior F1 score of 97%, underscoring its robust performance. Its ROC AUC score of 91% further demonstrates its excellent distinguishing power between classes. The model's low false positive rate of 1%, along with a standard deviation of 0.02, reaffirms its consistency and superior performance in managing overfitting and bias, common issues with individual decision trees. The ensemble approach of RF is adept at navigating intricate tasks with a multitude of variables, making it a choice contender for our security protocol.

The Decision Tree model, while not as accurate as the Random Forest with a mean accuracy of 86% and an F1 score of 84%, has a decent ROC AUC score of 80%. However, the model's relatively higher false positive rate of 5% indicates potential overfitting with complex trees. Its standard deviation of 0.01 indicates stable performance, although it struggles to compete with Random Forest's accuracy. The Naïve Bayes model, with a mean accuracy of 74% and an F1 score of 75%, has an ROC AUC score of 68%, indicating potential struggle with distinguishing classes. This could be due to the inherent assumption of feature independence in the model, often not applicable to real-world datasets. The false positive rate for this model is relatively high at 9%, but it maintains consistent performance with a standard deviation of 0.014. Lastly, the Logistic Regression model demonstrates stable performance with a standard deviation of 0.014. It achieves a mean accuracy of 76%, an F1 score of 78%, and an ROC AUC score of 70%, indicating decent accuracy and class distinguishing ability. However, it presents a slightly lower false positive rate of 8% compared to the Naïve Bayes model. While Logistic Regression is a sturdy model that excels when data can be linearly separated, it might falter when the data contains complex, non-linear relationships.

Nevertheless, while the Random Forest model outperforms the others, the choice of model will depend on the specific requirements and constraints of the given task. For our case, the choice of the supervised ML model is here random forest, which is also established by authors of [6] for IoT-based scenarios. Practically, it analyzes user data in real-time during every interaction, comparing it

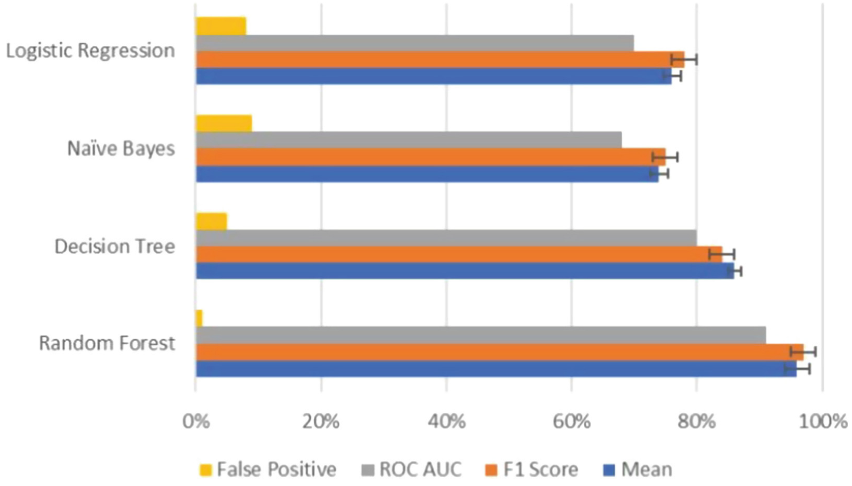


Fig. 6. Different Machine Learning Model's Accuracy Comparison using 10 Fold Cross Validation, F1 Score, ROC AUC, and Percentage of False Positive

with the patterns learned during training. Any detected aberration prompts the model to recommend that the user verify their certificate and private keys. This enhances security, rendering the process adaptive and resilient. These observations underline the necessity of selecting the correct model that aligns with the dataset's characteristics and the issue to be resolved. While the Random Forest model outperformed in this situation as can be seen in Fig. 7, under different circumstances, other models may surpass it. It is, therefore, essential to continuously test and validate the models with available data to ascertain peak performance.

In comparison to the state of the art methods of authenticating users in blockchain based models which we consider as our benchmark, the results were seen to be in the range of 16.62 ms and up to 272.89 ms [15], compared to our results of 10.095 ms in uploading authentication which is at its lowest a 60% decrease in authentication time. This shows that this method does enable a faster authentication time for regular users while maintaining the benefit of blockchain in connecting the industry to various clients' data points. All these results can be seen in Fig. 5b side by side on how well they perform compared to one another.

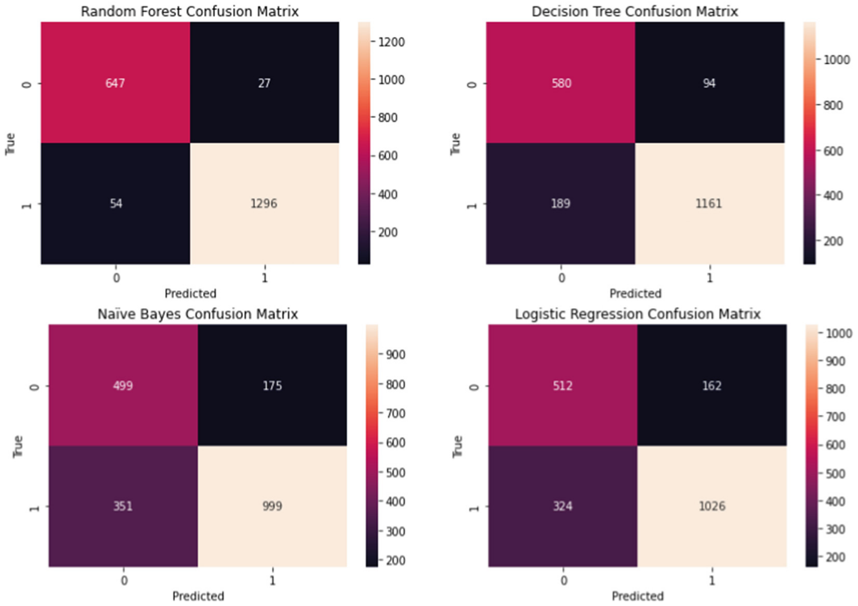


Fig. 7. Confusion Matrix for each Model for comparison

5 Conclusion and Future Work

The implementation of blockchain in IoT examines methods for establishing a private Ethereum network and devising a smart contract process that enables data sharing among stakeholders with access control in place. Here, we have designed and validated our proposed access control mechanism for a private Ethereum-based blockchain to securely manage IoT-based application data. Here, blockchain technology eliminates the need for a central authority by facilitating data transactions through an immutable, incorruptible distributed ledger. Furthermore, the study delves into the development of a smart contract system that facilitates the secure sharing of data among multiple stakeholders, incorporating effective access control measures. Thus, the proposed system effectively integrates the advantages of private blockchain technology and the Role-Based Access Control (RBAC) model, resulting in enhanced authentication efficiency and reduced authentication time.

According to the system design, some future implementations and additions to this work will incorporate IoT-level physical implementations to collect data from the real-world. Currently, the proposed model is being evaluated with synthesized IoT data. Future work will consist of installing Raspberry Pis and gathering IoT streaming data via them on a private blockchain, as well as evaluating the efficacy of scaling the entire infrastructure system.

Acknowledgements. This publication is based upon work supported by Khalifa University under Award No. FSU-2022-018.

References

1. Aarella, S.G., Mohanty, S.P., Kougianos, E., Puthal, D.: Fortified-edge: secure PUF certificate authentication mechanism for edge data centers in collaborative edge computing. In: Proceedings of the Great Lakes Symposium on VLSI 2023, pp. 249–254 (2023)
2. Almansoori, S., Alzaabi, M., Alrayssi, M., Puthal, D., Dutta, J., Shehhi, A.: Machine learning-based adaptive access control mechanism for private blockchain storage. In: 2023 IEEE 47th Annual Computers, Software, and Applications Conference (COMPSAC) (2023). https://doi.org/10.1109/COMPSAC57700.2023.00188
3. Butun, I., Österberg, P.: A review of distributed access control for blockchain systems towards securing the Internet of Things. IEEE Access **9**, 5428–5441 (2021). https://doi.org/10.1109/ACCESS.2020.3047902
4. Craß, S., Lackner, A., Begic, N., Mirhosseini, S.A.M., Kirchmayr, N.: Collaborative administration of role-based access control in smart contracts. In: 2022 4th Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), pp. 87–94 (2022). https://doi.org/10.1109/BRAINS55737.2022.9909116
5. Cruz, J.P., Kaji, Y., Yanai, N.: RBAC-SC: role-based access control using smart contract. IEEE Access **6**, 12240–12251 (2018). https://doi.org/10.1109/ACCESS.2018.2812844
6. Dutta, J., Puthal, D., Damiani, E.: AI-based block identification and classification in the blockchain integrated IoT. In: 2022 OITS International Conference on Information Technology (OCIT), pp. 415–421 (2022). https://doi.org/10.1109/OCIT56763.2022.00084
7. Han, D., Zhu, Y., Li, D., Liang, W., Souri, A., Li, K.C.: A blockchain-based auditable access control system for private data in service-centric IoT environments. IEEE Trans. Industr. Inf. **18**(5), 3530–3540 (2022). https://doi.org/10.1109/TII.2021.3114621
8. Kamboj, P., Khare, S., Pal, S.: User authentication using Blockchain based smart contract in role-based access control. Peer-to-Peer Networking Appl. **14**(5), 2961–2976 (2021). https://doi.org/10.1007/s12083-021-01150-1
9. Lee, Y., Lee, K.M.: Blockchain-based RBAC for user authentication with anonymity. In: Proceedings of the Conference on Research in Adaptive and Convergent Systems. ACM, September 2019. https://doi.org/10.1145/3338840.3355673
10. Liu, D., Dong, A., Yan, B., Yu, J.: DF-RBAC: dynamic and fine-grained role-based access control scheme with smart contract. Procedia Comput. Sci. **187**, 359–364 (2021). https://doi.org/10.1016/j.procs.2021.04.074, https://www.sciencedirect.com/science/article/pii/S1877050921008681, 2020 International Conference on Identification, Information and Knowledge in the Internet of Things, IIKI2020
11. Puthal, D., Malik, N., Mohanty, S.P., Kougianos, E., Das, G.: Everything you wanted to know about the blockchain: its promise, components, processes, and problems. IEEE Consum. Electron. Mag. **7**(4), 6–14 (2018). https://doi.org/10.1109/MCE.2018.2816299

12. Puthal, D., Yeun, C.Y., Damiani, E., Mishra, A.K., Yelamarthi, K., Pradhan, B.: Blockchain data structures and integrated adaptive learning: features and futures. IEEE Consum. Electron. Mag. (2023)
13. Sukhodolskiy, I., Zapechnikov, S.: A blockchain-based access control system for cloud storage. In: 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), pp. 1575–1578 (2018). https://doi.org/10.1109/EIConRus.2018.8317400
14. Swain, S., Puthal, D., Bertino, E.: CryptoCliqIn: graph-theoretic cryptography using clique injection. IEEE Intell. Syst. **37**(5), 59–65 (2021)
15. Thwin, T.T., Vasupongayya, S.: Blockchain-based access control model to preserve privacy for personal health record systems. Secur. Commun. Netw. **2019**, 1–15 (2019). https://doi.org/10.1155/2019/8315614
16. Wang, P., Xu, N., Zhang, H., Sun, W., Benslimane, A.: Dynamic access control and trust management for blockchain-empowered IoT. IEEE Internet Things J. **9**(15), 12997–13009 (2022). https://doi.org/10.1109/JIOT.2021.3125091

VXorPUF: A Vedic Principles - Based Hybrid XOR Arbiter PUF for Robust Security in IoMT

Md Ishtyaq Mahmud[1], Pintu Kumar Sadhu[1], Venkata P. Yanambaka[2](✉),
and Ahmed Abdelgawad[1]

[1] Central Michigan University, Mt Pleasant, MI, USA
[2] Texas Woman's University, Denton, TX, USA
vyanambaka@twu.edu

Abstract. The Internet of Medical Things (IoMT) is playing a pivotal role in the healthcare sector by allowing faster and more informed hospital care, personalized treatment, and medical solutions. Several authentication systems are used to safeguard the data and authenticate the devices, but some of them are inefficient and some of them have some limitations. A very effective and trustworthy solution for resource-constrained medical devices is provided by Physical Unclonable Functions (PUF) - based identity and authentication systems. This paper proposes VXorPUF, a Vedic Principles - Based Hybrid XOR Arbiter PUF. Modeling attacks were performed on the proposed architecture and an accuracy of 49.80% was achieved. Uniqueness, Reliability and Randomness were the figures of merit used to evaluate PUF. A further study was evaluated the uniformity of (m,n,p)-OAN-XOR-PUF, and a result of 43.75% was found, which is close to the ideal value of arbitrary PUF response.

1 Introduction

Due to recent technological breakthroughs and the advent of low-power, high-performance Internet of Things (IoT) devices, establishing an IoT ecosystem has become simple and straightforward. Several fields are being utilized by the IoT, including Smart Grid, Smart Self-driving Cars, IoT Farming, Smart Homes, Smart Healthcare, Military, Smart Cities, and Smart Industrial facilities. The demand for smart healthcare system using medical devices is high in the technology market besides other applications of IoT. IoMT has become an integral part of our daily life. IoMT devices are at the core of today's medical systems, where every medical equipment will be hooked up to the internet and supervised by healthcare practitioners [23]. In IoMT, highly sensitive personal health information is primarily collected; therefore, maintaining patients' privacy and security is crucial in helping to reduce the risk of negative consequences on their health, or in the worst-case scenario, causing their death [31]. With the global pandemic,

Published by Springer Nature Switzerland AG 2024
D. Puthal et al. (Eds.): IFIPIoT 2023, IFIP AICT 684, pp. 246–261, 2024.
https://doi.org/10.1007/978-3-031-45882-8_17

majority of the population has become health-aware and started using fitness trackers, health monitors and smart devices to improve their quality of life. This has given rise to an increased cyber attacks on the IoMT ecosystem [8]. Figure 1 shows the IoMT ecosystem where patient's medical data is collected through smart medical devices and sensors. Using the internet, applications for the IoMT are able to receive raw data collected by smart devices. The information is subsequently sent on to the medical practitioners and medical professionals, who respond to the people who require assistance. The data needs to be stored and pre processed, in some cases, through IoMT applications before sending it to the laboratories. In addition, there is a need to use additional in house or third party applications to assist with both the display of and analysis of the medical data.

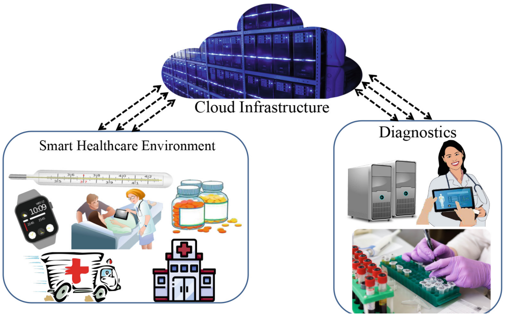


Fig. 1. The Internet of Medical Things (IoMT)

For IoT ecosystems, security and privacy are absolutely essential. A strong authentication architecture helps protect an IoT system from many threats. To secure the data and authenticate the devices, several IoT authentication schemes are used. However, some of them are ineffective and some of them have some limitations [11]. Although the IoMT devices are modest in size and lack the functionality to operate for intended job, constrained IoMT devices provide a wide range of functionalities. IoMT devices with resource-constraints are capable of collecting raw data from patients and transmitting it to healthcare practitioners for diagnosis and treatment [28]. The IMD's ecosystem is more promising because of low-power wireless technology [17] (RFID, NFC, BLE, WIFI, SigFox, Bluetooth, Ingenu, Weightless Zigbee, LoRa and Z-Wave) that require less battery life. These IoT devices are resource constrained devices with fewer microcontroller units (MCUs), less computational power, and less random access memory (RAM). They also require fewer functionality for wireless network protocols.

IoMT is regulated to increase clinical safety through the use of wireless medical sensor networks (WMSNs) [29]. In WMSNs, edge medical devices first measure user's data and send it to the medical practitioners through gate-way nodes(GWNs) for analyzing. A GWN with a large amount of computing power and memory capacity can serve as a useful medium between Sensor Nodes (SNs) and MPs because SNs are limited in resources and cannot perform sophisticated operations. PUF is a potential Hardware Assisted Security (HAS) modules that can generate device identification. For a lightweight and reliable IoT security system, we propose VXorPUF, a Machine Learning (ML) attack resistant Vedic Principles - Based Hybrid XOR Arbiter PUF. Rest of the paper is organized as follows: Sect. 2 gives an overview of PUF and ML attacks on PUF. Section 3 gives the related works in this area. The proposed PUF design is presented in Sect. 4 and the results are presented in Sect. 5. The conclusion and future directions of the research are presented in Sect. 6.

2 Physical Unclonable Functions

PUFs are the HAS primitives for reliable and lightweight security in resource-constrained environments, such as the IoT and IoMT devices. A PUF creates secret keys from intricate physical characteristics of a material that are challenging to duplicate or clone, rather than preserving secrets [30]. PUF takes in "challenges" as input and gives "responses" as outputs. PUF is categorized as "Silicon" and "Non - Silicon" PUFs, based on the manufacturing process and Security - Based PUFs depending on the Figures of Merit (FoM) of the responses generated.

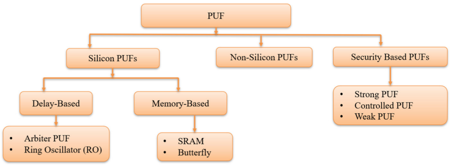


Fig. 2. Classification of PUFs

In [15], the phrase "silicon PUFs" was used to describe PUFs manufactured using traditional fabrication processes. Since silicon PUF does not require any modifications to the production process, it is undoubtedly the most simple PUF. These classes can be divided depending on the many sources of variation [42]. One such Silicon PUFs is Arbiter PUF. Figure 3 shows the architecture of traditional Arbiter PUF. Multiplexers are connected in series in an arbiter PUF. Due ot the manufacturing variations during the fabrication process of the Integrated Circuit (IC), each stage of multiplexer adds a different delay to the signal given at the input [16]. One of the major drawbacks of PUF for the metastablity of the delay flip-flop is that it has comparatively poorer reliability [41]. In order to prevent irreversible changes in the digital circuitry of a network, it is crucial to research the effects of aging on PUF. Digital circuits eventually fail due to the aging effect, which reduces performance. [19] they mentioned that due to the aging effect PUF response could be unreliable though there is no effect on randomness of PUF.

PUF is categorized as Weak, Strong and Controlled PUFs based on the FoMs of the generated responses. The challenges and responses of the PUF are pre-processed and post-processed in a controlled PUF to make it more reliable, and robust [37]. Veda PUF is one such controlled PUF proposed in [37]. It uses the ancient Vedic principles to pre-process and post-process the challenges and responses. Vedic literature has many important aspects to them, one being the ways they are recited. One among the 11 ways of reciting them are, "Ghana-patham". Considering three bits in binary, "b_1", "b_2', "b_3", they are repeated using the following in Ghanapatham:

$$S = [b_1, b_2][b_2, b_1], [b_1, b_2, b_3], [b_3, b_2, b_1], [b_1, b_2, b_3] \tag{1}$$

This is used to pre-process and post-process the keys in VedaPUF architecture.

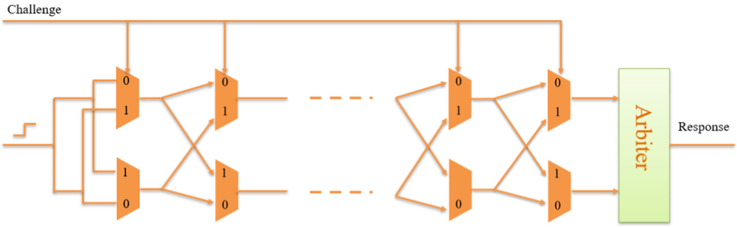


Fig. 3. Architecture of Arbiter PUF [4]

Machine Learning (ML) based modeling attack resistance is a significant need For PUF circuits. There have been reports of some Arbiter PUF compositions that have resisted modeling attacks and frequently need a lot of computer power for effective modeling [26]. ML, a highly parameterized strategy to produce predictions from observational data by employing specialized algorithms, is a key tool for conducting modeling threats [36]. In the recent past, ML has been utilized for PUF security research, where an attacker attempts to create a duplicate PUF model [5]. Attacker also makes an effort to accurately estimate the PUF response [24]. Modeling attack resistance is essential for PUFs because to ML's huge development and rising prominence in both science and industry.

3 Related Research

In today's digital revolution, Protecting patients' personal and medical information from unauthorized users, interpretation, and modification is a top priority. Security is becoming an increasing vital concern of makers and healthcare providers, because IMDs provides a significant services to the patients. Here is a review of some of the contributions the researchers made to the intelligent IoMT security framework.

Kwarteng et al. [14] mentioned some security threats of IMDs. DoS (Denial of Service) attack is one of them, this type of attack reduce the battery life expectancy. Reply Attack, try to change the status of IMDs by resend the identical request from a controller who already trusted. The researchers also discussed Software Injection, Man in the middle, and Side Channel attacks. Kautras et al. [12] addressed security protocols and constraints of IoT devices, when they adapt to the IoMT specialized network typologies. The researcher also identified alternative mitigation control that can be used to safeguard IoMT systems. Hatzivasilis et al. [6] mentioned BYOD (bring your own device) is another essential part of smart medical sectors that must be safeguarded in order to protect our patients' personal information.

Rahman et al. [22] demonstrated the significant vulnerability assessments for IoMT devices in WMSNs, as well as serious security flaws, in order to prevent hostile cyber-attacks. Furthermore, they discussed existing cryptographic authentication procedures to protect smart medical devices from cyber-attacks and discussed feasible solutions for addressing security weaknesses. Kumar et al. introduced cyber-attacks into IoMT networks, which are rapidly growing nowadays in hospital environment. They also introduced a solution for spotting cyber-attacks in fog-cloud infrastructure [13]. Nandy et al. presented a Swarm-Neural Network (Swarm-NN) technique for securing healthcare data while storing and sending information from the edge to the server with greater accuracy. This approach also detects threats and keeps track of the data's accuracy and parameters [20].

Almogren et al. [2] introduced sybil security risks, in which a single person creates several phony social media profiles in order to spread destructive misinformation. A fuzzy logic-based trust management (TM) technique has been presented by the researcher for mitigating the sybil security risk in medical environment and healthcare systems. Papaioannou et al. referred to a few hypothetical risks including potentially significant security mechanisms of IoMT devices [21]. Karmakar et al. [9] introduced a security design for forthcoming network virtualization platforms like OpenMANO. Furthermore, they explained how this security design used trusted healthcare network functionalities to authenticate IoMT devices. Wazid et al. explored some potential architecture and their implementations of IoMT ecosystems, as well as various malware attack and their symptoms. They also gave a comparison of the various malware detection systems that are currently in use, as well as some challenges and recommendations for future research [35].

Hardware Assisted Security (HAS) is a promising security solution for lightweight and robust security in IoMT. There are various security solutions proposed for the IoMT ecosystem [25,40]. PUF is a hardware assisted module to generate natural random numbers for cryptographic purposes [38]. PUF uses the manufacturing variations introduced during the fabrication of Integrated Circuits (IC) to generate the random numbers. The inputs and outputs of PUF are called "challenge - response pairs" (CRPs). PUF is used as a hardware security primitives for various applications, such as device authentication, communication, intellectual property protection, and so on [27].

Many designs of PUF were developed over the past few years for different applications. With the advancements in deep learning, PUF is vulnerable to modeling attacks [10]. Research has been going on to design a modeling attack resistant PUF [32]. Though many architectures were designed to resist the modeling attacks, the accuracy of such designs has always been over 70% [32]. With the high performance computing and developments in deep learning techniques, modeling attacks on PUF are becoming more aggressive and successful. This paper presents VXorPUF modeling attack resistant PUF for IoMT devices.

The researchers [34] prototyped the lattice PUF to secure IoT device against machine learning attacks. In Lattice PUF, the PUF logic proper required 45 slices, and the fuzzy extractor required 233 slices. In all of their attacks, they used a variety of ML models, including logistic regression, support vector machines, and deep neural networks. After analyzing their model they got the accuracy of above 50.24%. Subthreshold current array PUF (SCA-PUF) was proposed to resistant the machine learning attack [44]. In addition, amplifier-chain-based XOR-PUF [43] was also proposed. By employing 1 million CRPs as training datasets and an artificial neural network, the researchers achieved an accuracy of 50.70%. Furthermore, [1] the researcher demonstrated MPUF, which notably prevents ML attack. Their MPUF also performs better when it comes to randomness, reliability and uniqueness. After analyzing the machine learning model they got the prediction accuracy of 53.80%.

The researchers [26] introduced deep neural network based attack on wide variety of PUFs. They considered 64-bit and 128-bit arbiter PUF for modeling attack on PUFs. The attack is reasonably resilient to input dataset noise and computationally viable for the majority of real PUF designs. Though they need to be theoretically justify their proposed modeling attack on PUFs. Canaday et al. [3] proposed a uniqhe model-free ML attack, which model is based on deep learning based algorithms. Their framework against strong PUFs, which makes use of both collected CRP data from a particular target PUF and data gathered from additional PUF instances of the same type. The researchers also noted that their framework performed better than a number of other robust PUFs that are currently ML-resistant. Wang et al. [33] proposed a new ML-resistant robust PUF design. Their approach offers a way to combine inverted responses with regular ones, and that way ML algorithms are unable to generate a reliable model of the internal PUF.

4 Proposed VXorPUF: A Hybrid XOR Arbiter PUF for Robust Security in IoMT

The proposed VXorPUF uses the ancient Vedic principles at the core of the architecture to generate the modeling attack resistant CRPs. Veda-PUF, a controlled PUF architecture for robust lightweight design was proposed in [37].

VXorPUF uses the principle behind Veda-PUF as a controller mechanism to design a Hybrid XOR Arbiter PUF resistant to modeling attacks.

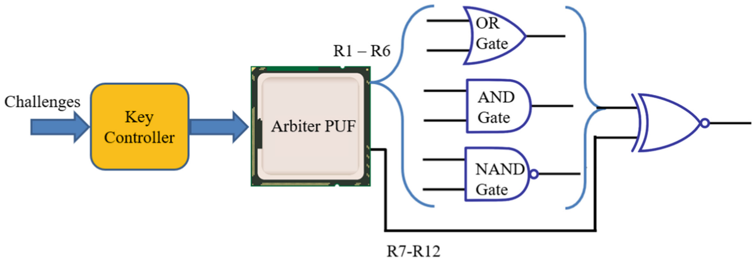


Fig. 4. Proposed VXorPUF Architecture

As shown in Fig. 4, The challenges given to the PUF are processed through a key-controller. The Veda theorem is presented [37] explicitly. This uses the vedic-principles to increase the key length to create 12 keys out of the challenge. Using the vedic principle, ghana, and jata, 3 bits of the challenge are repeated 13 times. For instance, consider three bits b_1, b_2, and b_3. Following is the expansion for the three bits:

$$s_1 = [b_1, b_2]\,[b_2, b_1]\,[b_1, b_2, b_3]\,[b_3, b_2, b_1]\,[b_1, b_2, b_3] \tag{2}$$

Equation 2 is used to generate 12 keys out of the challenge and give to the Arbiter PUF. Out of the 12 keys, 6 keys are selected and sent through AND, OR and NAND logic gates. The outputs of the logic gate are sent to an XOR gate for consolidation. The rest of the keys, 7–12, are passed to the XOR gate at the final stage. The final response is collected from the XOR gate and used for cryptographic purposes.

The proposed VXorPUF methods divided into three steps that is presented in Algorithm 1.

1. **Challenge Extension Using Key Controller**: The original challenge C_c will pass through key controller where Verdic principle will be applied. The controller will produce extended challenge R_c. The produced key will be divided into 12 partial 64-bit challenges which is represented by C_p. If the requirement of processing controller is valid then it will process further otherwise drop the challenge.
2. **PUF Response Generation**: Partial challenges C_p will act as input challenge C_a of the PUF. Each challenge will generate unique response R_a for each challenge. In this stage 12 responses will be generated using 64-bit Arbiter PUF.
3. **VXorPUF Response Production**: After inserting the PUF responses into the OR-AND-NAND block, PUF output is received. This block will generate 64-bit output using 12 64-bit responses. For example, to generate first output

Algorithm 1: Device Enrollment Phase

```
Input  : Challenges ($C_c$) to PUF in IoMT Device
Output: Responses from VXorPUF module $R_v$
Select the challenges for Key Controller $C_c$;
for each controller challenge $C_c$ do
    if Controller requirements met then
        $R_c \leftarrow C_c$;
        // $R_c$ = Controller response
        $R_c = C_p$;
        // Controller response($R_c$) devided into 12 challenges ($C_p$)
           for PUF
    else
        Drop the challenge;
for each challenge $C_p$ (12 times) do
    if PUF requirements met then
        $C_a \leftarrow C_p$;
        // $C_a$ = Arbitter PUF challenge
        $R_a = C_a$;
        // Arbiter PUF Response($R_a$) is considering as input challange
           ($C_a$) of Arbiter PUF
    else
        Drop the challenge;
for each VedaPUF input $R_i$ do
    $R_v \leftarrow$(OR$\oplus$AND$\oplus$NAND) $\leftarrow R_i$;
    // $R_i$ is the combined responses ($R_a$)
    Secure Database $\leftarrow R_v$, $C_a$;
    // $R_v$ = (OR$\oplus$AND$\oplus$NAND)-PUF output
    // Store the input challenge and VedaPUF output pair in secure
       database.
```

bit, bit-1 of first 2 responses will go to AND gate, next two responses first bit will go to NAND gate, first bit of fifth and sixth response will be used as input of OR gate. Three output of logic gates and first bit of response seven to twelve will be the input an XOR gate. The XOR gate will produce the first bit of the output. Consequently, rest bits will be generated and finally the input challenge of the key controller and the VedaPUF output will be saved in a secure database.

5 Experimental Results

The PUF is designed using a Field Programmable Gate Array (FPGA). A 64-bit arbiter PUF was employed among other PUFs, and it can produce CRPs, satisfying the necessary PUF requirements. Xillinx Basys 3 FPGA was used to prototype the VXorPUF. One FPGA was attached to a Raspberry Pi in the experimental setup to create an MD. FPGAs' PUFs were used to implement the challenges, and linked Raspberry Pis were employed to compile the responses. The output bit for the arbitrator PUF is determined by comparing the amount of time needed to traverse a signal. The work was implemented with the help of Google Colab, BASYS3 FPGA, and Raspberry Pi 4 B+. The CRPs are collected from the PUF module. 500000 keys were selected as a challenge and 500000 responses were collected from the VXorPUF.

The core component used in the VXorPUF prototype was a 64-bit Arbiter PUF. The challenges and the responses were 64-bits in length. Besides modeling attack resistance, the PUF has to satisfy the FoM for the keys to be used for cryptographic applications. This paper considers three FoMs, uniqueness, reliability and randomness.

5.1 Uniqueness

A uniqueness of PUF is the ability of the module to generate a unique key at the module. A key generated by a PUF for a respective challenge is unique to the module and cannot be generated by a different challenge. Hamming distance is used to calculate the uniqueness of the keys generated from the PUF.

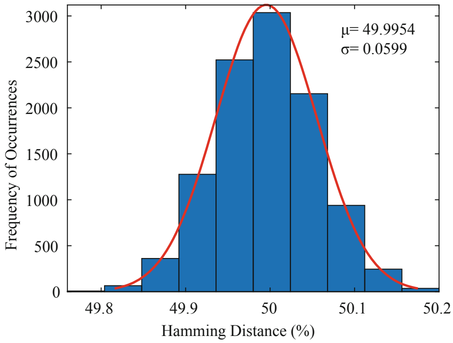


Fig. 5. Uniqueness of PUF

Figure 5 shows the uniqueness of VXorPUF. The ideal hamming distance of a PUF is 50%. As shown in the figure, the proposed PUF design has a mean uniqueness of 49.9% and a standard deviation of 0.05%. These keys show a value close to the ideal values showing a strong key generation.

5.2 Randomness

Randomness of the keys are the number of 1 and 0 bits in the generated key. A uniform distribution of 1 and 0 in the final key shows a strong resistant to prediction and a better uniqueness. The ideal value of randomness of the PUF keys is 50%. Figure 6 shows the randomness of the keys generated by the VXorPUF. As shown in the figure the mean randomness is 49.9% with a standard deviation of 6.2%.

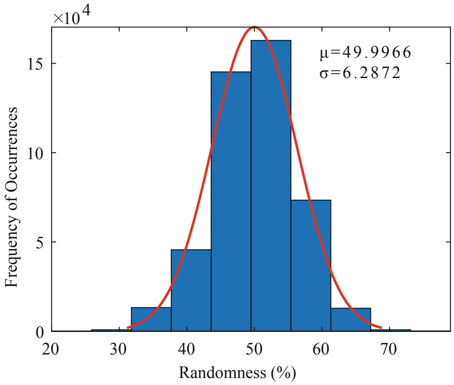


Fig. 6. Randomness of PUF

5.3 Reliability

Reliability of PUF is the ability to generate a consistent set of CRPs under various conditions. To test the reliability of the PUF, initially, the same challenge is repeated to test the response for multiple runs. The same test is repeated for multiple challenges considered during the testing phase. For given challenges, the VXorPUF showed a reliability of the 99.9%. The PUF module is tested for reliability under temperature variations. Multiple temperature points were considered, from 50°F through 150°F at 15°F intervals. At each stage, the keys were collected to test for reliability. The VXorPUF showed a reliability of 99.9% with a consistent generation of CRPs.

5.4 Machine Learning Method

Various architectures of PUF were generated through the PUF module and

In this work, 64 bit challenges were generated utilizing an arbiter PUF employing a BASYS 3 FPGA. The data was generated at the lab. For the purposes of making training, validation, and testing, the dataset was divided 80:20. The first 80% of training & validation will be used for training, with the rest for validation.

Table 1. Data for Machine Learning

ML Stages	Amount of Data	Training	Testing
Pre-Processing	500000	400000	100000
Final Stage	455732	364585	91147

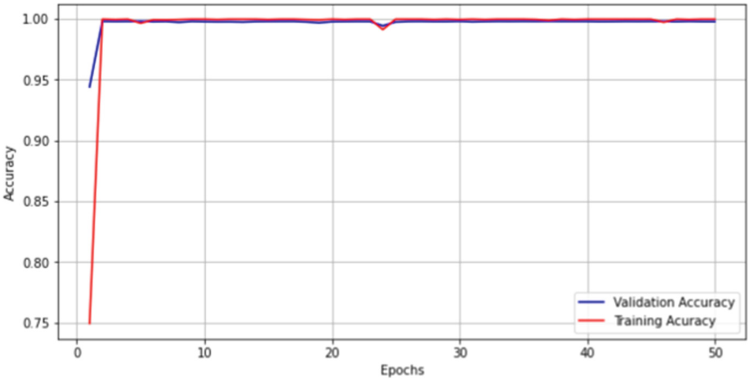


Fig. 7. Accuracy of Pre-Processing Stage

The Machine Learning (ML) environment is created using Google Colab pro+ and runs totally in the cloud. The environment setup makes advantage of the NVIDIA Tesla K80, T4, and P100 GPU that is built into colab. Google colab Pro+ uses a 52 Gb high-RAM runtime to create an ML environment.

In this research multilevel binary classification were used. The widely used pattern recognition and classification algorithm logistic regression is most often applied to classification tasks. A logistic regression model was applied. Models based on this architecture consist of four layers, with rectified linear units (ReLU) acting as activation functions in each layer. 50 epochs were run to evaluate the performance of the models and locate the point at which the performance of the validation data leveled off. Different optimizer which were “Adam”, “SGD”, “RMSProp”, “Adadelta”, “Adagrad”, “Adamax”, “Nadam” tried to get the best performance of the machine learning model. Also, various activation function (“ReLU”, “Sigmoid”, “ELU”) were used.

1. Pre-Processing Stage: Fig. 7 shows the training and validation accuracy of pre-processing stage. At this stage, the input and output data were both 64 bits. Accuracy is around 99.78% using activation function ReLU and optimizer Adam. ReLU and Adam outperformed other optimizer and activation functions when such factors were taken into account.
2. Final Stage: Fig. 8 depicts the last stage’s training and validation accuracy. After submitting the 64 bit response to the AON-XOR operation, 64 bit data were obtained and used for machine learning at this stage. With the activation function ReLU and Adam optimizer, accuracy is around 49.80%. At this stage,

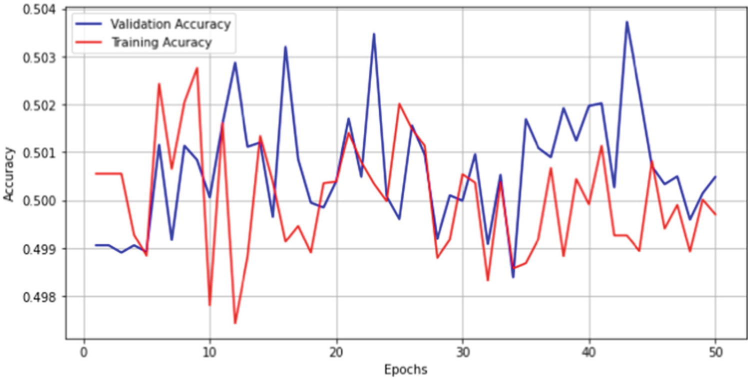


Fig. 8. Accuracy of Final Stage

different activation functions and optimizer were tested to compare them and forecast the most accurate model.

To compare the performance of the proposed VXorPUF, the machine learning modeling attack was performed on the Arbiter PUF before the post processing stage of the keys. An accuracy of 49.80% was achieved using the ReLU activation function and Adam optimizer. ReLU and Adam outperformed other optimizer and activation functions compared to the other optimizer. Figure 8 and Fig. 7 has shown the performance of machine learning for the final stage and pre-processing stages, respectively.

Table 2. Analysis the Accuracy of Final Stage for Different Optimizer and Activation function

Accuracy			Optimizer
ReLU	ELU	Sigmoid	
49.80%	49.85%	50.00%	Adam
49.85%	49.88%	50.00%	SGD
49.94%	49.85%	50.23%	RMSProp
50.19%	50.14%	49.90%	Adadelta
49.93%	49.82%	49.89%	Adagrad
50.18%	50.11%	50.22%	Adamax
50.17%	50.05%	49.95%	Nadam

Table 2 displays the accuracy of final stage while focusing on different activation functions with optimizer. The best performance in this case is provided by the Adam optimizer with the activation function ReLU.

Table 3. Comparison Analysis of PUF

References	Randomness	Uniqueness	ML Models Accuracy
[34], 2020	49.98%	50%	50.24%
[44], 2019	52.8%	49.9%	60%
[43], 2021	—	49.92%	50.72%
[7], 2019	49.7%	47.49%	69.41%
[1], 2022	95%	49.76%	53.8%
Our Work	49.995%	49.9966%	49.80%

Table 3 demonestrate the comparison analysis of PUF model. Where we have considered the metrics of uniqueness, randomness and Machine learning model accuracy of PUF for comparing previous work with our work. They proposed [43] amplifier-chain based XOR-PUF where they got the ML prediction accuracy of 50.72%. They [1] used MRAM-PUF for their research work, where uniformity response id around 95% though the p-value is higher than 0.01. Which indicate that their MPUF is highly random. They proposed [7] XOR-Inverter ROPUF, where they got the ML prediction accuracy of 69.41%.

Our ML models accuracy is more encouraging when compared to other researchers' work; we obtained a 49.80% accuracy rate, indicating that our proposed VxorPUF is more trustworthy in machine learning attack on PUF. Additionally, we came close to optimal values for randomness and uniqueness while considering our proposed VxorPUF. The uniformity of the OR- AND- XOR - PUF (OAX-PUF) was reported as 50% in [39], while our proposed VxorPUF achieved a uniformity of 43.75%.

6 Conclusion and Future Works

As patient personal information is transferred and emergency medical care is required, the healthcare environment's security and privacy are of utmost importance. Using Vedic principle, we have demonstrated that PUF provides greater dependability and security in resource-constrained smart medical devices in healthcare system as compared to generic PUF-based authentication procedure. We have analyzed three Figures of Merit (FoMs), Uniqueness, Randomness, and Reliability of VxorPUF, and got the promising outcomes of Veda-PUF for resource-constrained devices. In addition, our proposed model preformed better and achieved the machine learning accuracy of 49.80%, which indicating that the use of VxorPUF has increased the security of PUFs against machine learning attacks. In future study, we might consider bulk amount of PUF keys to evaluate how resistant the PUF against machine learning attack.

Acknowledgments. A version of the current paper is published in [18].

The authors would like to thank Mr. Dendukuri Swaminatha Sarma for his support during the research on Vedas.

References

1. Ali, R., Zhang, D., Cai, H., Zhao, W., Wang, Y.: A machine learning attack-resilient strong PUF leveraging the process variation of MRAM. In: Express Briefs, IEEE Transactions on Circuits and Systems II (2022)
2. Almogren, A., Mohiuddin, I., Din, I.U., Almajed, H., Guizani, N.: Ftm-iomt: fuzzy-based trust management for preventing sybil attacks in internet of medical things. Proc. IEEE Internet Things J. **8**(6), 4485–4497 (2020)
3. Canaday, D., Barbosa, W.A., Pomerance, A.: A novel attack on machine-learning resistant physical unclonable functions. In: 2022 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), pp. 25–28. IEEE (2022)
4. Gao, Y., Al-Sarawi, S.F., Abbott, D., Sadeghi, A.R., Ranasinghe, D.C.: Modeling attack resilient reconfigurable latent obfuscation technique for PUF based lightweight authentication. arXiv preprint arXiv:1706.06232 (2017)
5. Gassend, B., Lim, D., Clarke, D., Van Dijk, M., Devadas, S.: Identification and authentication of integrated circuits. Concurr. Comput. Pract. Exp. **16**(11), 1077–1098 (2004)
6. Hatzivasilis, G., Soultatos, O., Ioannidis, S., Verikoukis, C., Demetriou, G., Tsatsoulis, C.: Review of security and privacy for the Internet of Medical Things (IoMT). In: Proceedings of 2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS), pp. 457–464. IEEE (2019)
7. Hazari, N.A., Oun, A., Niamat, M.: Analysis and machine learning vulnerability assessment of XOR-inverter based ring oscillator PUF design. In: 2019 IEEE 62nd International Midwest Symposium on Circuits and Systems (MWSCAS), pp. 590–593 (2019). https://doi.org/10.1109/MWSCAS.2019.8885037
8. Hodgkiss, J., Djahel, S.: Securing fuzzy vault enabled authentication in body area networks-based smart healthcare. IEEE Consum. Electron. Magaz. **11**(1), 6–16 (2022). https://doi.org/10.1109/MCE.2020.2991387
9. Karmakar, K.K., Varadharajan, V., Tupakula, U., Nepal, S., Thapa, C.: Towards a security enhanced virtualised network infrastructure for Internet of Medical Things (IoMT). In: Proceedings of 2020 6th IEEE Conference on Network Softwarization (NetSoft), pp. 257–261. IEEE (2020)
10. Khalafalla, M., Gebotys, C.: PUFs deep attacks: enhanced modeling attacks using deep learning techniques to break the security of double arbiter PUFs. In: Design, Automation and Test in Europe Conference and Exhibition (DATE), pp. 204–209 (2019). https://doi.org/10.23919/DATE.2019.8714862
11. King, J., Awad, A.I.: A distributed security mechanism for resource-constrained IOT devices. Informatica **40**(1) (2016)
12. Koutras, D., Stergiopoulos, G., Dasaklis, T., Kotzanikolaou, P., Glynos, D., Douligeris, C.: Security in iomt communications: a survey. Sensors **20**(17), 4828 (2020)
13. Kumar, P., Gupta, G.P., Tripathi, R.: An ensemble learning and fog-cloud architecture-driven cyber-attack detection framework for IoMT networks. Comput. Commun. **166**, 110–124 (2021)
14. Kwarteng, E., Cebe, M.: A survey on security issues in modern implantable devices: solutions and future issues. Smart Health 100295 (2022)
15. Lim, D., Lee, J., Gassend, B., Suh, G., van Dijk, M., Devadas, S.: Extracting secret keys from integrated circuits. IEEE Trans. Very Large Scale Integrat. Syst. **13**(10), 1200–1205 (2005). https://doi.org/10.1109/TVLSI.2005.859470

16. Mahmud, M.I., Abdelgawad, A., Yanambaka, V.P.: A deep analysis of hybrid-multikey-PUF. arXiv preprint arXiv:2304.04381 (2023)
17. Mahmud, M.I., Abdelgawad, A., Yanambaka, V.P., Yelamarthi, K.: Packet drop and RSSI evaluation for LoRa: an indoor application perspective. In: Proceedings of IEEE 7th World Forum on Internet of Things (WF-IoT), pp. 913–914 (2021). https://doi.org/10.1109/WF-IoT51360.2021.9595288
18. Mahmud, M., Sadhu, P., Yanambaka, V., Abdelgawad, A.: Vxorpuf: a vedic principles - based hybrid XOR arbiter PUF for robust security in IoMT. Preprints.org (2023030499) (2023)
19. Maiti, A., McDougall, L., Schaumont, P.: The impact of aging on an FPQA-based physical unclonable function. In: 2011 21st International Conference on Field Programmable Logic and Applications, pp. 151–156. IEEE (2011)
20. Nandy, S., Adhikari, M., Khan, M.A., Menon, V.G., Verma, S.: An intrusion detection mechanism for secured IoMT framework based on swarm-neural network. IEEE J. Biomed. Health Inform. **26**(5), 1969–1976 (2021)
21. Papaioannou, M., et al.: A survey on security threats and countermeasures in internet of medical things (IoMT). Trans. Emerg. Telecommun. Technol. **33**(6), e4049 (2022)
22. Rahman, M., Jahankhani, H.: Security vulnerabilities in existing security mechanisms for IoMT and potential solutions for mitigating cyber-attacks. In: Jahankhani, H., Kendzierskyj, S., Akhgar, B. (eds.) Information Security Technologies for Controlling Pandemics. ASTSA, pp. 307–334. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-72120-6_12
23. Razdan, S., Sharma, S.: Internet of medical things (IoMT): overview, emerging technologies, and case studies. In: IETE Technical Review, pp. 1–14 (2021)
24. Rührmair, U., Sehnke, F., Sölter, J., Dror, G., Devadas, S., Schmidhuber, J.: Modeling attacks on physical unclonable functions. In: Proceedings of the 17th ACM Conference on Computer and Communications Security, pp. 237–249 (2010)
25. Sadhu, P., Yanambaka, V.P., Abdelgawad, A., Yelamarthi, K.: NAHAP: PUF-based three factor authentication system for internet of medical things. IEEE Consum. Electron. Magaz. 1 (2022). https://doi.org/10.1109/MCE.2022.3176420
26. Santikellur, P., Bhattacharyay, A., Chakraborty, R.S.: Deep learning based model building attacks on arbiter PUF compositions. Cryptology ePrint Archive (2019)
27. Satamraju, K.P., Balakrishnan, M.: A secured healthcare model for sensor data sharing with integrated emotional intelligence. IEEE Sens. J. **22**(16), 16306–16313 (2022). https://doi.org/10.1109/JSEN.2022.3189268
28. Shoaran, M., Haghi, B.A., Taghavi, M., Farivar, M., Emami-Neyestanak, A.: Energy-efficient classification for resource-constrained biomedical applications. IEEE J. Emerg. Select. Top. Circuits Syst. **8**(4), 693–707 (2018)
29. Siddiqi, M.A., Tsintzira, A.A., Digkas, G., Siavvas, M.G., Strydis, C.: Adding security to implantable medical devices: can we afford it? In: Proceedings of EWSN, pp. 67–78 (2021)
30. Suragani, R., Nazarenko, E., Anagnostopoulos, N.A., Mexis, N., Kavun, E.B.: Identification and classification of corrupted PUF responses via machine learning. In: 2022 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), pp. 137–140. IEEE (2022)
31. Vaiyapuri, T., Binbusayyis, A., Varadarajan, V.: Security, privacy and trust in IoMT enabled smart healthcare system: a systematic review of current and future trends. Int. J. Adv. Comput. Sci. Appl. **12**(2), 731–737 (2021)

32. Wang, S.J., Chen, Y.S., Li, K.S.M.: Modeling attack resistant PUFs based on adversarial attack against machine learning. IEEE J. Emerg. Select. Top. Circuits Syst. **11**(2), 306–318 (2021). https://doi.org/10.1109/JETCAS.2021.3062413
33. Wang, S.J., Chen, Y.S., Li, K.S.M.: Modeling attack resistant PUFs based on adversarial attack against machine learning. IEEE J. Emerg. Select. Top. Circuits Syst. **11**(2), 306–318 (2021)
34. Wang, Y., Xi, X., Orshansky, M.: Lattice PUF: a strong physical unclonable function provably secure against machine learning attacks. In: 2020 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), pp. 273–283. IEEE (2020)
35. Wazid, M., Das, A.K., Rodrigues, J.J., Shetty, S., Park, Y.: IoMT malware detection approaches: analysis and research challenges. IEEE Access **7**, 182459–182476 (2019)
36. Wisiol, N., Thapaliya, B., Mursi, K.T., Seifert, J.P., Zhuang, Y.: Neural network modeling attacks on arbiter-PUF-based designs. IEEE Trans. Inf. Forens. Secur. **17**, 2719–2731 (2022)
37. Yanambaka, V.P., Mohanty, S.P., Kougianos, E., Baniya, B.K., Rout, B.: Veda-PUF: a PUF based on vedic principles for robust lightweight security for IoT. In: IEEE International Symposium on Smart Electronic Systems (iSES), pp. 400–405 (2021). https://doi.org/10.1109/iSES52644.2021.00097
38. Yanambaka, V.P., Mohanty, S.P., Kougianos, E., Puthal, D.: PMsec: physical unclonable function-based robust and lightweight authentication in the internet of medical things. Proc. IEEE Trans. Consum. Electron, **65**(3), 388–397 (2019). https://doi.org/10.1109/TCE.2019.2926192
39. Yao, J., et al.: Design and evaluate recomposited or-and-XOR-PUF. IEEE Trans. Emerg. Top. Comput. (2022)
40. Yoon, S., Kim, B., Kang, Y.: Multiple PUF-based lightweight authentication method in the IoT. In: International Conference on Information and Communication Technology Convergence (ICTC), pp. 1198–1200 (2021). https://doi.org/10.1109/ICTC52510.2021.9620972
41. Zalivaka, S.S., Ivaniuk, A.A., Chang, C.H.: Reliable and modeling attack resistant authentication of arbiter PUF in FPGA implementation with trinary quadruple response. IEEE Trans. Inf. Forens. Secur. **14**(4), 1109–1123 (2018)
42. Zerrouki, F., Ouchani, S., Bouarfa, H.: A survey on silicon PUFs. J. Syst. Architect. **127**, 102514 (2022)
43. Zhang, J., et al.: A 4t/cell amplifier-chain-based XOR PUF with strong machine learning attack resilience. IEEE Trans. Circuits Syst. I Regul. Pap. **69**(1), 366–377 (2021)
44. Zhuang, H., Xi, X., Sun, N., Orshansky, M.: A strong subthreshold current array PUF resilient to machine learning attacks. IEEE Trans. Circuits Syst. I Regul. Pap. **67**(1), 135–144 (2019)

Easy-Sec: PUF-Based Rapid and Robust Authentication Framework for the Internet of Vehicles

Pintu Kumar Sadhu[1](✉) and Venkata P. Yanambaka[2]

[1] Central Michigan University, Mt Pleasant, MI, USA
sadhu1pk@cmich.edu
[2] Texas Woman's University, Denton, TX, USA

Abstract. With the rapid growth of new technological paradigms such as the Internet of Things (IoT), it opens new doors for many applications in the modern era for the betterment of human life. One of the recent applications of the IoT is the Internet of Vehicles (IoV) which helps to see unprecedented growth of connected vehicles on the roads. The IoV is gaining attention due to enhancing traffic safety and providing low route information. One of the most important and major requirements of the IoV is preserving security and privacy under strict latency. Moreover, vehicles are required to be authenticated frequently and fast considering limited bandwidth, high mobility, and density of the vehicles. To address the security vulnerabilities and data integrity, an ultralight authentication scheme has been proposed in this article. Physical Unclonable Function (PUF) and XOR function are used to authenticate both server and vehicle in two message flow which makes the proposed scheme ultralight, and less computation is required. The proposed Easy-Sec can authenticate vehicles maintaining low latency and resisting known security threats. Furthermore, the proposed Easy-Sec needs low overhead so that it does not increase the burden of the IoV network. Computational (around 4 ms) and Communication (32 bytes) overhead shows the feasibility, efficiency, and also security features are depicted using formal analysis, Burrows, Abadi, and Needham (BAN) logic, and informal analysis to show the robustness of the proposed mechanisms against security threats.

Keywords: Internet of Things · Security · Privacy · Internet of Vehicles · Physical Unclonable Function · Encryption · Authentication Protocol

1 Introduction

With the rapid advancement and development of the IoT, both people and devices are being interconnected now-a-days. The IoT has become an inseparable part of our daily life by making integration of physical and digital communities. This trends and development are evidencing *industry 4.0* which was coined in 2011.

Published by Springer Nature Switzerland AG 2024
D. Puthal et al. (Eds.): IFIPIoT 2023, IFIP AICT 684, pp. 262–279, 2024.
https://doi.org/10.1007/978-3-031-45882-8_18

The forth industrial revolution will bring advancement in the manufacturing process by successive prediction, control, maintenance, and integration of physical build (such as sensors, actuators, complex machinery etc.) and cyber parts (such as network, software etc.). Industry 4.0 is categorized as: IoT, cyberphysical systems, fog computing, cloud computing, Big Data analytics, robotics, augmented and virtual reality, cybersecurity to semantic web technologies, and additive manufacturing [1]. Industry is doing huge investment and according to Gartner report, by 2021 devices consisting sensors and actuators will make spend around $2.5 million [2]. Furthermore, according to the Gartner report [3,4], the IoT is one of the top ten fastest growing and emerging technology with the largest business potential as there will be 20 times more smart devices by 2023. It also suggested that the revenue of the IoT market will be declined by 3% in 2020 which will be rebounded in 2021. In the era of industrial 4.0, for creating beneficial impacts the IoT is transforming and revolutionizing into a wide range of fields, such as the IoV, wearables to robots, smart city, urban planning, power, and so on [5].

Among these applications, the IoV is gaining attention of academia, researchers, industrialists, and so on. Over the last few years in vehicular network and road, the number of autonomous vehicles (AV) is rising sharply in general, and it is estimated that it may cross two billion within the next 10–20 years [6]. The increment trend takes part in the introduction of the intelligent transportation system and related technologies that can enable services, such as smart road sign management, traffic management, efficient insurance policy, toll collection, passenger management, etc. According to a report Association for Safe International Road Travel, nearly 1.25 million people die in road crashes each year which makes an average of 1,287 deaths a day. Another report shows that 1.3 million deaths every year and over 50 million people are injured in car accidents and it is possible to avoid 60%–70% accidents [7]. Human error is the cause in 90% of cases. The IoV is a potential solution to enhance the driving experience by improving convenience and road safety [8]. As every devices are smart and also connected, the network has been targeted to become under attack such as cyber and physical attacks. The cyber attack on Ukraine's power infrastructure caused outages of 225,000 consumers in 2015. Also, regular cyber attacks are attempted on U.S. power grids and other systems. So, network of the IoT or the industry 4.0 such as the IoV demands robust and secure system [2]. Table 1 shows acronyms and symbols are used in this article.

The rest of the paper is organized as follows: Sect. 2 discusses the prior research related to the Smart Vehicle and the IoV security and privacy, Sect. 3 presents the proposed Easy-Sec architecture. The results of the proposed framework are presented in Sect. 4 and the conclusion and future directions are proposed in Sect. 5.

2 Related Work

Many researchers are working to secure the IoV network as it is growing and it depends on many things including human life. The IoV network demands

Table 1. Acronyms and Symbols used in the Current Paper

Notation	Description
Easy-Sec	PUF-Based Rapid and Robust Authentication Framework
IoV	Internet of Vehicles
VANET	Vehicular ad-hoc Network
V2X	Vehicle to Everything
V2V	Vehicle-to-Vehicle
V2I	Vehicle-to-Infrastructure
V2S	Vehicle-to-Sensors
V2N	Vehicle-to-Network
V2P	Vehicle-to-Pedestrian
AV	Autonomous Vehicle
RSU	Roadside Unit
RG	RSU Gateway
CS	Cloud Server
SDB	Secure Database
PUF	Physical Unclonabale Function
C	Challenge
R	Response
V_{PID}	Pseudo Identity of AV (PUF)
PID_{New}	New Pseudo Identity of AV (PUF)
N_v, N_s	Random Nonce
R_C	Response for Challenge C
R_{C+I}	Response for Challenge (C+I)
R^K	K-bit Response for Challenge C
$(Y)_R$	Encryption of message Y using key R
$R(Y)$	Decryption of message Y using key R
K, I	Random Integer Number
Z	Function of Random Integer Number
$\|\|$	Concatenation
$\oplus$	XOR Operation
$\in$	Store Operation
$F_{nl}()$	Any Non-linear Function

a secure authentication protocol that requires low complexity, less resources, faster authentication. In this section, literature review of existing authentication schemes of the IoV network will be discussed.

In 2017 [9], an authentication scheme for large scale IoV was proposed. It used a certificate that is loaded in AV before registration by a certificate authority. Private-public key would be issued during registration time if the certificate seems valid. This key was used for encryption. ID was not anonymous in this case and also after changing the RSU area, fake certificates could be used to forgery vehicles. A certificate-less scheme [10] was proposed to avoid certificate storage in TA and AV. To hide the secret key, it used two random values which made the messages unlinkability. It assumed that discrete algorithm was intractable and also it was stated that in future work, the vulnerabilities and limitations of the work would be removed to achieve security and privacy requirements.

So far discussed authentication schemes are applicable for centralized systems whereas blockchain is used for decentralized systems. A blockchain based solution to ensure security and privacy of the IoV network in [11]. It preserved data from being exposed and modified. A debit-credit based blockchain scheme was proposed in [12] to avoid the cold start of new vehicles or users. But this work required protecting signatures and their resources. A high resourceful adversary could compromise the system. An incentive mechanism, where multiple vehicles bid to complete a task using their resources, was developed in [3]. Moreover, the bidding system was avoided in case of emergency conditions where multiple vehicles make a cluster. This scheme took a reactive approach to resist attack instead of a proactive approach. Furthermore, this scheme did not depict inter-vehicle communication for clustering. Vehicles calculated credibility considering the distance between vehicles in the scheme of [13]. This work used Bayesian Inference Model and uploads ratings to RSUs. This work was suitable against limited resourceful attackers. Also, it did not resist reply attacks, man-in-the-middle attacks, and introduces high overhead. The framework in [14] used SDN enabled OBU for effective network management and also fog computing for avoiding frequent handovers. However, this work required to be more focused on data transmission trust.

3 Proposed Authentication Framework

This section presents the proposed authentication protocol for the application of the IoV. The proposed authentication framework consists of the following six main system components:

- Drivers/Passengers: Passengers are the primary users in the IoV system who are different individual entities residing in the autonomous vehicle to reach the desired destination. It is required to share real-time information of route such as traffic, which demands strong privacy the in IoV application.
- Autonomous Vehicles (AV): AVs which are embedded with ECUs to grab signal, traffic information and computation etc. Moreover, AVs are equipped with PUF for authenticating vehicle in the IoV network.
- Roadside Unit (RSU): RSU is generally described as vehicular communication systems. RSU is a transceiver, resides on the roadside, which sends or receives signal from AVs, pedestrians etc. Furthermore, an RSU operating in a particular location where it is licensed to operate. It supports storage for memory allocation, processor that runs applications for computing capabilities, network capabilities such as 4G/LTE or 5G and also GPS receiver that support secure communications with passing vehicles, other field equipment, and centers. A PUF is integrated into the RSU. It collects messages from AVs and send to RG after combining those.

- RSU Gateway (RG): RG provides coverage of a certain location and RSUs of the coverage area connected with the RSU gateway. RSUs are authenticated with RSU gateway for connection. A PUF is integrated to the RG. An RG combines the messages of its serving RSUs and send to Cloud Server for computation, verification and other tasks.
- Cloud Server (CS): Cloud server is the decision maker for establishing communication between entities. It authenticates AVs, pedestrians, RSUs etc. before accepting data. Moreover, it is a memory device for storing traffic related information in the IoV application.
- Secure Database (SDB): SBD is secured storage for keeping CPR set of AVs, RSUs etc. which is required for authentication by cloud server.

Each AV wakes up from inactivity mode, it tries to sends & receives traffic information from the IoV network. Before connecting to the IoV network, it must go through authentication process to identify whether it is legitimate vehicle or user. Each AV must go through two phases for being part of the IoV network. Initially, it is required to be registered and then perform mutual authentication phase.

3.1 Overview of PUF-Based Ultalight Authentication Framework

Figure 1 shows the proposed PUF based security paradigm. As shown in the figure, AVs are the end devices. Each AV is connected to an RSU and each RSU is connected to an RG. An RG is connected to a number of RSUs and combined coverage area of those RSUs is the serving area of the RG. There are multiple RGs which are connected with a cloud server. When an AV wants to join the IoV network, it will communicate with the CS through the nearest serving RSU, and RG for mutual authentication. After successful authentication, the AV can be part of the network to send and receive required traffic information. For mutual authentication, the CS will ask the AV to generate a response for a selected challenge. If the response matches with the one stored on the SDB, authentication will be successful. A session key will then be shared with the AV for further communication. The AV does not need to authenticate again within the RG coverage area. When the AV changes RG serving area, session keys are required to be updated which avoids further mutual authentication. The symbols which are used in this authentication scheme are presented in Table 1.

3.2 Assumptions

The following assumptions are considered for secure and successful mutual authentication using proposed framework:

- Each AV and RSU, RG are embedded with PUF chips and at the time of AV's registration, AVs which are embedded with PUF will go through CRP generation step in the registration phase through secure channel.

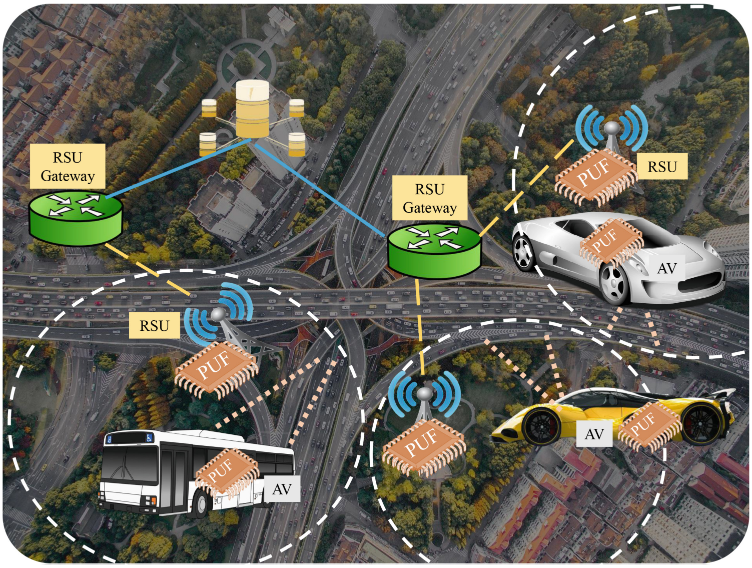


Fig. 1. Architecture of the Proposed PUF Based Ultalight Authentication Scheme in the Application of the IoV

– There is a secure connection between CS and SDB. SDB is the only trusted center of CS for storing.
– The IDs, PIDs, CRPs of AVs, RSUs and RGs are stored in the SDB of the CS during the registration phase.
– No shared keys exists either between AVs and RSU; or RSUs and RGs; or RGs and CS.
– RSUs, RGs are already authenticated with CS for communication.
– AV does not maintain continuous connection with the RSU, RG and CS, instead it operates in wake-sleep cycles for better energy efficiency. When a user needs to go to a place, it wakes up and establish secure session by authenticating mutually.
– It is considered that the PUFs which are used in this scheme are noise resistant and perform in the same way in every environment and life span. Like [15,16], there are many noise resistant PUFs have been developed in recent times to ensure the reliability which can deal with environmental issues, voltage fluctuations, wide temperature ranges, pressure and humidity etc.

3.3 PUF-Based AV Registration Phase

When a client purchased a new AV and want to enroll in the IoV network, it is first required to go through registration phase. Every AV which needs to be registered in the IoV network must have a integrated PUF module. Registration process needs to be performed through a secure channel and secure environment and the PUF module in the vehicle satisfies the required characteristics of PUF which is discussed in the Sect. 1. Figure 2 shows the registration process of the AV for the proposed authentication scheme. Both AV and CS have an integrated PUF module.

A challenge "$C1$", selected will be given to the PUF at CS and a response, "$R1$" is generated. This response "$R1$" is sent to the AV which is given as a challenge for the integrated PUF. The response, "R" generated at the PUF in AV is sent back to the CS. This "R" becomes the challenge for the PUF at the AV and generates a response, "$R2$". The response $R2$ is stored in the SDB along with the initial challenge. To maintain the privacy of the AV, a pseudo random identity is sent to the AV for future communications. The control flow of the registration process of a AV is represented by Fig. 2. Here, Challenge-Response relation is depicted by >> sign. For instance, $C2>> R2$ represents $C2$ as Challenge (input) and $R2$ as Response (output). On the other hand, → sign indicates that transmitted output will act as input to the receiver. For example, $R \rightarrow C2$ shows R will be transmitted and it will be input $C2$ of the CS.

Because of unique process variation of chips, each CRP of a PUF will act as an unique fingerprint of the vehicle. For storing a CRP, it is required to perform the CRP generation multiple times to check the reliability of the module. This process is repeated for other challenges and corresponding hash values are computed; then the pair is stored in the SDB for the PUF. It is noted that no CRP is stored in the AV in this process. AV will only generate response when a challenge is provided to the AV. The AV registration flow is shown in Algorithm 1. AV is introduced into the network after the successful registration.

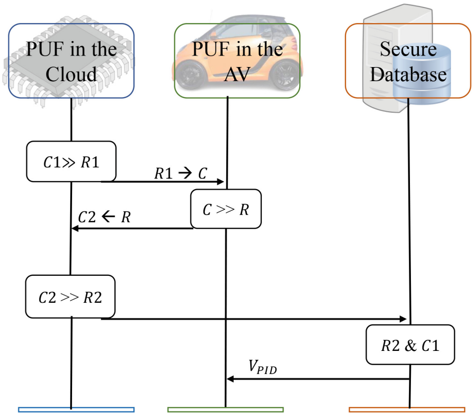


Fig. 2. Easy-Sec Vehicle Registration

Algorithm 1: AV Registration

```
    CS:
        $C1 >> R1$ ▷ In the CS, $C1$ will act as a challenge and will generate response $R1$
    CS → AV { $R1$, i.e. $C$ }  ▷ The CS will send $R1$ to AV. The $R1$ is same as challenge
  $C$ in the AV
        $C >> R$
    AV → CS { $R$, i.e. $C2$ }
        $C2 >> R2$
    CS → SDB
        $\in \{C1, R2\}$                                   ▷ Storing CRP in the SDB
    SDB → AV
        $\in \{V_{PID}\}$ ▷ After storing CRPs, a $V_{PID}$ will be assigned to the AV and will be
  stored to the SDB
```

3.4 Easy-Sec: Proposed Authentication Scheme

The proposed authentication scheme is presented in Fig. 3. It shows that both server and vehicle authenticate each other communicating through the RSU and RG. The flow of verification using the proposed framework is represented by Fig. 4. For brevity, the message flow of RSUs and RGs are not shown in the Fig. 4 as RSUs pass messages from AVs and RGs pass message from RSUs. The authentication process can be divided into 3 phases. Authentication flow is shown in Algorithm 2.

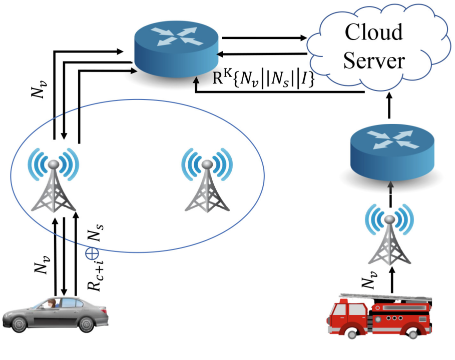


Fig. 3. Easy-Sec Authentication Protocol

As stated earlier, it is assumed that PUF based RSU and RG are already been authenticated using CRP communication.

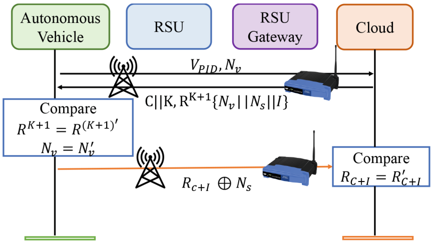


Fig. 4. Easy-Sec Authentication Verification

1. **Authentication Session Initiation from AV:** When an AV wakes up and initiates a connection to the network, it sends V_{PID} and a nonce N_v to RSU for starting a session. RSU passes this packet to the RG and RG to CS. CS will identify the AV using V_{PID} and ID from its stored SDB. The data flow from AV to RSU to RG to CS is illustrated as **Phase-1** of **Authentication process**.
2. **Verification of CRP from CS:** During this phase, AV will fetch the challenge and random nonce from CS. CS will send R^{K+1} encrypted nonce N_v, its own generated nonce N_s and a random number to find the challenge. When AV gets the data from CS through RG and RSU, it generates the response using the challenge C and find out $K+1$ bit to decrypt the data to find out information. After decryption, it checks whether the nonce it matches or not. If AV finds out the same nonce in the decrypted data, then it verifies the CS. The server verification is presented in **Phase-2** of **Authentication process**.
3. **AV Authentication Confirmation:** In the phase-3, AV generates response of challenge $C{+}I$ and shares with nonce N_s to CS via RSU and RG after doing XOR operation. CS verifies $R_{(C+I)}$ and N_s after performing reverse XOR operation. If all these values match, then CS will identify AV as authenticated entity and establish a session key for further communication with RSUs within the serving region of RG. The entire process of this phase is demonstrated in **Phase-3** of **Authentication process**.

3.5 Session Key Update

When an AV reaches the end of the coverage area of the serving RG, then it is required to update session key to connect with a RSU of the moving RG. Session key update process excludes future authentication requirement.

Red signal indicates that the signal strength of the serving RSU is becoming weak and green signal indicates that AV is getting strong signal from the moving RSU. The flow of session key update is represented in the Fig. 5. The session key update process can be divided into 2 phases.

Algorithm 2: Secure Authentication Process

```
Phase-1: Authentication session initiation from AV
AV → RSU $\{V_{PID} \,||\, N_v\}$  ▷ The AV initiates authentication by sending concatenation of $PID$ of AV and a random nonce
RSU → RG $\{V_{PID} \,||\, N_v\}$
RG → CS $\{V_{PID} \,||\, N_v\}$
if $V_{PID} == V_{PID'}$ then
    Continue  ▷ The CS will the validity of the AV $PID$
else
    Invalid Client
end
Phase-2: Verification of CRP from CS
CS:
    $F2_{AV} = (\ N_v \,||\, N_s \,||\, I\ )_{R^{K+1}}$  ▷ The CS will encrypt using $(K+1)$ bit of response $R$ for challenge $C$
CS → RG $\{C \,||\, K,\ F2_{AV}\}$  ▷ The CS will send concatenation of challenge $C$ and $K$ along with encrypted result
RG → RSU $\{C \,||\, K,\ F2_{AV}\}$
RSU → AV $\{C \,||\, K,\ F2_{AV}\}$
    $C \longrightarrow R^{K+1}$  ▷ The AV will generate $(K+1)$ bit response using challenge $C$
    $\{N_v,\ N_s,\ \mathrm{I} = R^{K+1}\ (\ F2_{AV}\ )\ \}$  ▷ The AV will decrypt the encrypted result to find $N_v$, $N_s$, and $I$
if $N_v == N_v^{'}$ then
    Valid Server  ▷ Authenticity of the CS will checked by verifying $N_v$
else
    Invalid Server
end
Phase-3: AV Authentication Confirmation
AV:
    $C{+}I \longrightarrow R_{C+I}$  ▷ Response will be generated using challenge $(C+I)$ in the AV
    $F3_{AV} = F_{nl}(R_{C+I} \oplus N_s)$  ▷ XOR result of generated response and the CS shared nonce will be sent to the CS through the IoV network
AV → RSU $\{F3_{AV}\}$
RSU → RG $\{F3_{AV}\}$
RG → CS $\{F3_{AV}\}$
    $\{R_{C+I} \oplus N_s\} = F3_{AV}$
    $Z = R_{C+I} \oplus N_s$
if $Z == Z^{'}$ then
    Authenticated & Establish Session Key  ▷ The CS will verify the XOR result of response and nonce
else
    Authentication Failed
end
```

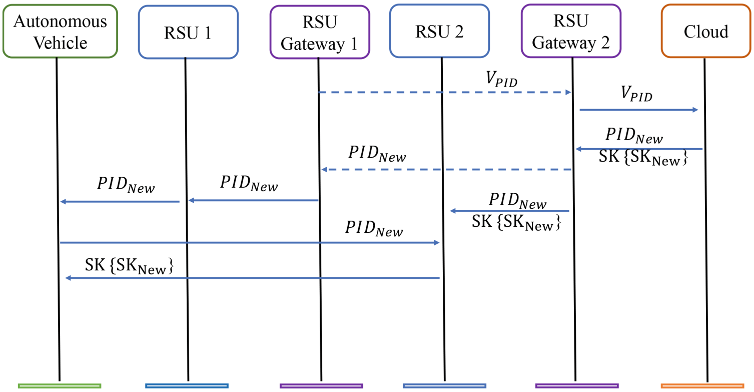


Fig. 5. Procedure of Session Key Update

1. **New Session Key Generation:** When RG finds that an AV is about to cross it serving area, then it will initiate session key update process. It will send V_{PID} to the new RG which is RG2 in the figure to. RG2 will communicate with CS for new session key and new PID. CS will check the existence of the PID and will generate PID_{New} and session key SK_{New}. Then CS will share PID_{New} and encrypted SK_{New} to RG2. After getting information from CS, RG2 will share PID_{New} to RG1 and both PID_{New} & encrypted SK_{New} to the new RSU which is RSU2 in the figure. AV will get PID_{New} via RSU1 and this PID_{New} will be valid for 1 min so that an adversary can not attempt to impersonate the AV. These process is presented in **Phase-1** of **Session key update process**.
2. **New Session Key Receiving by AV:** In this phase, AV will initiate communication with RSU2 by sending $PID_{New}+1$. Then, RSU2 will share the encrypted SK_{New} with AV. Using current session key, AV will decrypt the message and find out the new session key for making communication in the new RG serving area. The demonstrated process is shown in **Phase-2** of **Session key update process**.

4 Experimental Results and Security Analysis

4.1 Experimental Setup

There are many PUF architectures which can generate CRP following the required characteristics. In this work, 64 bit arbiter PUF was used among various PUFs. PYNQ^{TM} Z2 FPGA which is based on Xilinx Zynq C7Z020 SoC was used for PUF implementation. Also, Xilinx BASYS3 FPGA was used to build the 64-bit Arbiter PUF. An arbiter PUF is a delay-based PUF that generates

Algorithm 3: Session Key Update Process

```
Phase-1: New Session Key Generation
RG1 → RG2 $\{V_{PID}\}$    ▷ RG1 initiates session key update process
RG2 → CS $\{V_{PID}\}$
CS → RG2 $\{PID_{New}, (\ SK_{New}\ )_{SK}\}$    ▷ The CS shares a new $PID$ of the AV and encrypts a session key using current session key
RG2 → RG1 $\{PID_{New}\}$    ▷ RG2 shares the new $PID$ of the AV to RG1
RG2 → RSU2 $\{PID_{New}, (\ SK_{New}\ )_{SK}\}$
Phase-2: New Session Key Receiving by AV
AV → RSU2 $\{PID_{New}+1\}$    ▷ The AV requests for the session key
RSU2 → AV $\{\ (\ SK_{New}\ )_{SK}\}$    ▷ RSU shares the encrypted session key
AV:
  $\{SK_{New} = SK\ (\ SK_{New}\ )\ \}$    ▷ The AV decrypts the session key to get the new session key
```

a response based on two delay-lines time differences. Each box from $A0$ to $A63$ represents a unit of two delay-lines to generate a bit.

Raspberry Pi 4 B+, PYNQ Z2 FPGA, and BASYS3 FPGA were used for implementing the work. The experimental setup of the proposed Easy-Sec is shown in the Fig. 6. In the figure, it is shown that FPGA is being used as PUF of AV and Raspberry Pi is being worked as AV which are connected together. On the other hand, another Raspberry Pi is working as CS which has a secure database. When authentication request is being sent to CS by AV, CS transmits message which is encrypted using R^{K+1} and in response, AV shares R_{C+I} with nonce of CS. Using the full process, both CS and AV verification will be done so that each can identify whether other end is legitimate or not.

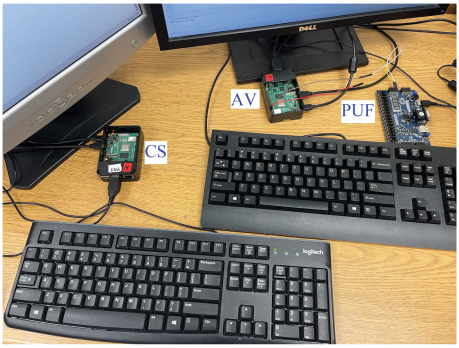
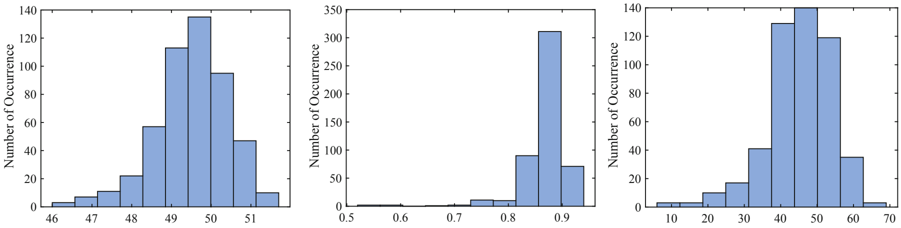


Fig. 6. Experimental Setup of the proposed protocol: Easy-Sec

4.2 Results

In this section, performance of the proposed authentication protocol will be analyzed. First, the performance of PUF will be presented. Figure 7 shows the characteristics of the 64-bit PUF that were used in the proposed authentication protocol. The performance was measured using 500 CRPs. It was found that the PUF showed 49.52% Uniqueness, 86.85% Randomness, and 45.67% inter-HD which can be identified as good performance. Moreover, the PUF showed 100% reliability. Furthermore, the reliability of PUF was measured at 15°F intervals from 30°F to 150°F temperature scale. The PUF showed robustness as each temperature 100% reliability was found.



(a) Uniqueness (b) Randomness (c) Inter-HD

Fig. 7. Figures of Merit of 64-bit PUF

Now, performance analysis of the proposed Easy-Sec will be shown. As shown in the authentication section, it is divided into three phases. The data presented here are based on 20 collected samples. Total computational time was 4.18ms to complete all the 3 phases. Among 3 phases, phase-2 is required much time due to decryption and other processes. Table 2 shows computational time of both AV and CS side for all phases. Figure 8 represents computational time requirement for each phases on the proposed Easy-Sec.

Table 2. Computational Time at both AV and CS

Item	AV Time (ms)	CS Time (ms)	Total Time (ms)
Phase-1	0.04	0.54	0.58
Phase-2	1.51	1.41	2.92
Phase-3	0.41	0.27	0.69
Total	1.96	2.22	4.18

Moreover, a network of 10 vehicles (Raspberry Pis) was created to check the computation time and scalability of the proposed framework. Computational

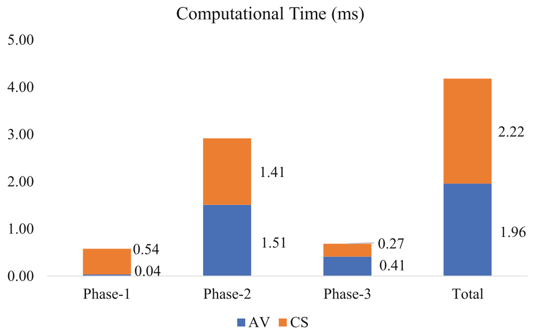


Fig. 8. Computational Time of Different Phases of Easy-Sec

time per device does not increase (decrease with a smaller amount) with the increased number of vehicles. The trend of computational time is presented in Fig. 9.

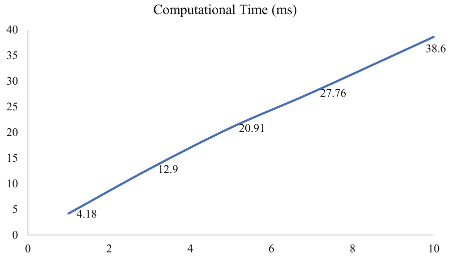


Fig. 9. Computational Time of Different Phases of Easy-Sec

CRP generation was required for 2 times in the authentication protocol. In this experiment, FPGA was used for responses generation after feeding challenges from Raspberry PI. Table 3 presents communication time between Raspberry PI & FPGA and response generation time. As responses will be generated in the same SoC, only response generation time is considered in computational time.

For calculating communication overhead in the current work, 64 bits were used as PID and random nonce was considered as 16 bits. Figure 10 shows the distribution of message flow of each step.

Table 4 shows communication overhead of the proposed Easy-Sec.

As per data flow, total communication overhead of the proposed scheme is 32 bytes. If SHA-256 is used in the encryption process, then total overhead

Table 3. CRP Generation and Communication Time

Item	Time (ms)
Response Generation	0.4
Raspberry PI and FPGA Communication	35.0
Total	35.4

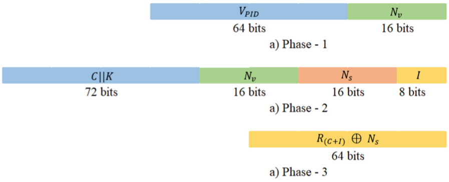


Fig. 10. Message flow during each phase of Easy-Sec

Table 4. Communication Overhead

Item	Communication Overhead (bytes)
Phase-1	10
Phase-2	14
Phase-3	8
Total	32

will be 59 bytes. Communication overhead depends on PID length, types of encryption, random nonce length, size of K-bit etc. Hence, final communication overhead will be based on selection of above parameters. Furthermore, for session key update when AV changes RG area, it will take 0.5 ms to extract the new session key as here only decryption of new session key using current session key is required as computation. For communication overhead, it is also low as AV is required to send new PID to new RSU where it will receive encrypted session key. Communication overhead will be as per selection of PID size and encryption mechanism.

Table 5 shows the comparative performance analysis among different proposed authentication schemes. From the table, it is evident that the proposed scheme is better than other existing authentication frameworks with respect to performance. Also, the proposed scheme is secured against known security threats which are shown in the security analysis section.

Table 5. Performance Comparison

Item	Year	Communication Overhead (bytes)	Computational Cost (ms)	Remarks
Li et al. [10]	2019	408	0.5*	Only message generation and verification are considered; High performance Xeon CPU is used instead of OBU for simulation
Han et al. [17]	2021	**	15.7	Should have higher overhead due to sending multiple parameters
Thumbur et al. [18]	2020	184	27	Many cryptographic operations
Alladi et al. [19]	2020	**	22	Communication overhead should be higher as it sends keys, IDs, nonce, timestamps etc. few times
Aman et al. [20]	2020	24*	**	Communication overhead is 102 bytes by calculating as this paper
Javaid et al. [21]	2020	512	**	It is a blockchain-based authentication scheme
This Paper		32	5	Simple scheme with low cost and overhead

* - Full authentication process is not considered
** - Information is not provided

5 Conclusion and Future Directions

In this paper, a secure and ultralight authentication scheme is proposed for verifying the AV to send/receive traffic information and firmware update process. It is an efficient and secure PUF-based authentication framework for the application of the IoV. The proposed scheme is free from complex certificate management, key storage problem. As the authentication of both CS and AV is done by using two message flow, this technique simplifies the verification time, computational cost, communication overhead, bandwidth requirement and storage space at AV, RSU and RG. The proposed authentication protocol is shown to prevent from disrupting the security features by both informal security analysis and BAN logic. Performance analysis shows that the proposed authentication scheme is more efficient compared to similar state-of-the authentication schemes in terms of security, computational, and communication point of view. Hence, the proposed PUF-based authentication scheme is more feasible for the IoV environment.

Though this paper shows very low computational time and communication overhead, it will be targeted to further lowering time and cost by reducing CRP generation timeline and other optimization schemes. Moreover, blockchain will be introduced to decentralize and compare the performance.

Acknowledgments. A version of this paper is presented in [22]. The authors would like to thank Dr. Saraju Mohanty and Dr. Elias Kougianos for their support during research.

References

1. Rikalovic, A., Suzic, N., Bajic, B., Piuri, V.: Industry 4.0 implementation challenges and opportunities: a technological perspective. IEEE Syst. J. 1–14 (2021)
2. Garg, S., Kaur, K., Kaddoum, G., Raymond Choo, K.-K.: Toward secure and provable authentication for internet of things: realizing industry 4.0. IEEE Internet Things J. **7**(5), 4598–4606 (2020)
3. Yin, B., Yulei, W., Tianshi, H., Dong, J., Jiang, Z.: An efficient collaboration and incentive mechanism for internet of vehicles (IoV) with secured information exchange based on blockchains. IEEE Internet Things J. **7**(3), 1582–1593 (2019)
4. Gartner Top 10 Strategic Technology Trends for 2020. https://www.gartner.com/smarterwithgartner/gartner-top-10-strategic-technology-trends-for-2020/. Accessed 08 Aug 2021
5. Liang, Y., Samtani, S., Guo, B., Zhiwen, Y.: Behavioral biometrics for continuous authentication in the internet-of-things era: an artificial intelligence perspective. IEEE Internet Things J. **7**(9), 9128–9143 (2020)
6. Jia, D., Kejie, L., Wang, J., Zhang, X., Shen, X.: A survey on platoon-based vehicular cyber-physical systems. IEEE Commun. Surv. Tutor. **18**(1), 263–284 (2015)
7. Zadobrischi, E., Damian, M.: Vehicular communications utility in road safety applications: a step toward self-aware intelligent traffic systems. Symmetry **13**(3), 438 (2021)
8. Mejri, M.N., Ben-Othman, J., Hamdi, M.: Survey on VANET security challenges and possible cryptographic solutions. Vehicul. Commun. **1**(2), 53–66 (2014)
9. Guo, L., et al.: A secure mechanism for big data collection in large scale internet of vehicle. IEEE Internet Things J. **4**(2), 601–610 (2017)
10. Li, J., Ji, Y., Raymond Choo, K.-K., Hogrefe, D.: CL-CPPA: certificate-less conditional privacy-preserving authentication protocol for the internet of vehicles. IEEE Internet Things J. **6**(6), 10332–10343 (2019)
11. Wazid, M., Bera, B., Das, A.K., Mohanty, S.P., Jo, M.: Fortifying smart transportation security through public blockchain. IEEE Internet Things J. (2022)
12. Liu, K., Chen, W., Zheng, Z., Li, Z., Liang, W.: A novel debt-credit mechanism for blockchain-based data-trading in internet of vehicles. IEEE Internet Things J. **6**(5), 9098–9111 (2019)
13. Yang, Z., Yang, K., Lei, L., Zheng, K., Leung, V.C.M.: Blockchain-based decentralized trust management in vehicular networks. IEEE Internet Things J. **6**(2), 1495–1505 (2018)
14. Gao, J., et al.: A blockchain-SDN-enabled internet of vehicles environment for fog computing and 5G networks. IEEE Internet Things J. **7**(5), 4278–4291 (2019)
15. Xuyang, L., Hong, L., Sengupta, K.: CMOS optical PUFs using noise-immune process-sensitive photonic crystals incorporating passive variations for robustness. IEEE J. Solid-State Circuits **53**(9), 2709–2721 (2018)
16. Chuang, K.-H., Bury, E., Degraeve, R., Kaczer, B., Linten, D., Verbauwhede, I.: A physically unclonable function using soft oxide breakdown featuring 0% native BER and 51.8 fJ/Bit in 40-nm CMOS. IEEE J. Solid-State Circuits **54**(10), 2765–2776 (2019)

17. Han, M., Zhu, M., Cheng, P., Yin, Z., Haixin, Q.: Implementing an efficient secure attribute-based encryption system for IoV using association rules. Symmetry **13**(7), 1177 (2021)
18. Thumbur, G., Srinivasa Rao, G., Vasudeva Reddy, P., Gayathri, N.B., Koti Reddy, D.V.R., Padmavathamma, M.: Efficient and secure certificateless aggregate signature-based authentication scheme for vehicular ad hoc networks. IEEE Internet Things J. **8**(3), 1908–1920 (2020)
19. Alladi, T., Chakravarty, S., Chamola, V., Guizani, M.: A lightweight authentication and attestation scheme for in-transit vehicles in IoV scenario. IEEE Trans. Veh. Technol. **69**(12), 14188–14197 (2020)
20. Aman, M.N., Javaid, U., Sikdar, B.: A privacy-preserving and scalable authentication protocol for the internet of vehicles. IEEE Internet Things J. **8**(2), 1123–1139 (2020)
21. Javaid, U., Aman, M.N., Sikdar, B.: A scalable protocol for driving trust management in internet of vehicles with blockchain. IEEE Internet Things J. **7**(12), 11815–11829 (2020)
22. Sadhu, P., Yanambaka, V.P., Mohanty, S.P., Kougianos, E.: Easy-sec: PUF-based rapid and robust authentication framework for the internet of vehicles. Comput. Sci. 27. arXiv preprint arXiv:2204.07709 (2022)

IoT for Smart Healthcare (SHC)

FortiRx: Distributed Ledger Based Verifiable and Trustworthy Electronic Prescription Sharing

Anand Kumar Bapatla[1], Saraju P. Mohanty[1](✉), and Elias Kougianos[2]

[1] Department of Computer Science and Engineering, University of North Texas, Denton, USA
anandkumarbapatla@my.unt.edu, saraju.mohanty@unt.edu

[2] Department of Electrical Engineering, University of North Texas, Denton, USA
elias.kougianos@unt.edu

Abstract. A paper-based prescription signed by the prescriber to authorize dispensing of medication is typically used in traditional healthcare. Such systems are prone to many issues like medication errors, latency, and lack of integration with other healthcare systems. Hence, Electronic prescription (E-prescription) systems are being used as alternatives to overcome these issues. Even though E-prescription systems provide the advantage of recording and maintaining patient medication history but still face issues such as system crashes, latency due to their centralized architectures, prone to many security threats like identity theft and unauthorized patient record access and modifications. Lack of standardization can also make such E-prescription systems not interoperable, which may lead to information fragmentation or delays in the processing of prescriptions. Hence, there is still a need for making these E-prescription systems more secure, reliable, and cost-effective for wide-range adaptation. Blockchain is one such technology that can add additional layers of security to the existing E-prescription systems by providing tamper-proof records of all transactions which will help in ensuring the authenticity and integrity of prescriptions. Blockchain can also help in better management of patients' privacy while patients still have full control over their health data. Blockchain usage can also enhance interoperability and reduce prescription abuse. The proposed application FortiRx makes use of the Ethereum blockchain platform and leverages smart contracts for implementing business logic. Cyphertext-Policy Attribute-Based Encryption (CP-ABE) is used in the proposed application to create and manage access-control mechanisms and ensure Health Insurance Portability and Accountability Act (HIPPA) compliance. The proposed system has been implemented and analyzed for security, reliability, and adaptability in a real-time environment.

Keywords: Smart Healthcare · Healthcare Cyber-Physical System (H-CPS) · Electronic Prescription · Blockchain · Distributed Ledger · Ethereum · Smart Contracts · Attribute Based Encryption · Cyphertext-Policy Attribute Based Encryption

Published by Springer Nature Switzerland AG 2024
D. Puthal et al. (Eds.): IFIPIoT 2023, IFIP AICT 684, pp. 283–301, 2024.
https://doi.org/10.1007/978-3-031-45882-8_19

1 Introduction

Paper-based prescriptions have been one of the preferred ways of sending medication instructions by physicians for a long time. Handwritten prescriptions are often difficult to read and susceptible to fraud by duplication. It is also a time-consuming process that requires patients to physically deliver the prescription to pharmacies. It also causes issues while integrating with Electronic Health Records (EHR) and makes it difficult to keep track of patient's medication history. All these issues with traditional paper-based prescriptions cause medication errors [1]. Medication errors are defined as preventable events which cause improper usage of medication by patients and can lead to patient harm. These medication errors can occur at multiple aspects of medication systems such as while prescribing the drugs, while entering prescription information into the electronic systems, while preparing the prescription for dispense, or while consuming the medication by patients [8]. The World Health Organization (WHO) determined medication errors are the leading cause of patient harm and account for up to $42 billion annually [16,21,24]. In order to reduce the number of medication errors, electronic prescription systems have been put into place to make the whole process computerized to reduce human errors. Initially, the patient requests a refill, or the physician creates a new prescription record based on the diagnosis of the patient and enters it into the electronic record system. Electronic Medical Record (EMR) or Electronic Health Record (EHR) system then generates an electronic prescription transaction and with the prescription along with the physician information to a centralized E-prescription system. E-prescription then verifies the authenticity of the prescription before sending it to the authorized pharmacies from which the patient will be able to pick it up. Any refill requests will be generated by the pharmacy and sent back to the physician using the E-prescribing system and notify the patient for pickup. The working of the E-prescribing system can be clearly seen in Fig. 1. Other entities like government agencies U.S. Food and Drug Administration (FDA), Centers for Medicare and Medicaid Services (CMS), Healthcare Information Exchanges (HIEs) along with Pharmacy Benefit Managers (PBMs) are also involved in E-prescribing systems. Due to the complex nature of interactions, those are not shown in Fig. 1.

E-prescription is the ability to use the computerized system by healthcare providers to create, manage and transmit prescription data to pharmacies. The E-prescription system increases the legibility of prescriptions thereby reducing the likelihood of errors. It also increases efficiency by automating most of the processes and reducing the administrative processing needed to issue and manage paper-based prescriptions. By automating the processes and reducing medical errors, costs associated with medical errors can also be avoided. It also makes it easy to integrate with EMR systems which can help in managing patient health records more efficiently. Although E-prescription systems provide a variety of benefits compared to the paper-based approach, it still faces many issues which need to be addressed.

The centralized architecture of the E-prescription can lead to latency in processing large amounts of information and even sometimes lead to a Single Point of Failure (SPOF). They are even prone to many other security threats that may lead to data privacy and security issues [26]. This lack of standardization between such centralized systems can lead to problems during integration with Electronic Healthcare Record Sys-

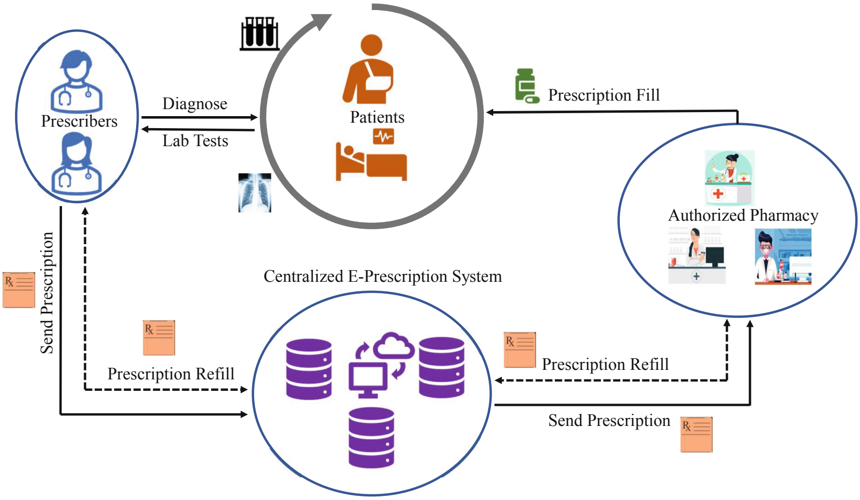


Fig. 1. E-Prescribing System Working

tems (EHRs). The cost of deployment and maintenance of such systems is also a major hurdle for adopting. The complexity of such systems is another problem for users of e-prescription systems.

The rest of the paper is organized as follows: Sect. 2 presents possibility of using blockchain or distributed ledger for e-prescription in H-CPS. Section 3 gives an overview of prior related research. Section 4 talks about the novel features of the proposed FortiRx system. Section 5 discussed the preliminaries and Sect. 6 describes the architecture of the proposed FortiRx system. Section 7 discusses proposed algorithms for uploading and managing prescription information. Section 8 describes the implementation of the proposed FortiRx system. Section 9 provides the analysis details and Sect. 10 provides conclusions along with future research aspects.

2 Blockchain as a Solution for Robust E-Prescription

Blockchain is a type of distributed ledger technology that helps in recording and storing information in a secure, transparent, and distributed manner in Peer-to-Peer (P2P) network. Blockchain is initially designed for digital assets in Bitcoin [15] but this technology has revolutionized and shown potential use-cases in many domains including patient EHR Management [9,10], supply chain management in the pharmaceutical industry and medicine manufacturing [4,13] etc. The main components of the blockchain consist of Distributed Ledger (DL), Nodes, Transactions, and consensus protocol. Block ledger generally consists of hash-connected blocks which have both header with all metadata and body with actual transactions. Header and body are implemented so that the light nodes which doesn't want to store all the transaction data can prune the body and just store the header information and still verify any transaction. The structure of the ledger varies for different implementations and the most prominent structures are blockchain which is a linear structure of blocks and Decentralized Acyclic Graph (DAG) which uses graph structure for scalability of the network. All the participants in the P2P network are called nodes and are classified as light node, miner node, and full nodes based on their roles and responsibilities. Light nodes are the nodes with limited storage and computational capabilities which don't store the entire history of the transaction data, usually, these are the participant nodes that try to utilize blockchain infrastructure to perform transactions. Mining nodes are special nodes that have the large computational power and usually compete to solve a hard mathematical problem to win a chance of adding a new block to the ledger. Miners are awarded block rewards combined with transaction fees from the transactions included in the block generated by them. Full nodes are responsible for storing complete copies of the ledger including all transaction data and verifying both transactions and blocks which ensures the security and integrity of the blockchain. Usually, full nodes are not compensated with any fees or rewards. Communication in a P2P network without delegation of centralized authority is prone to issues of disagreement which is described as a Byzantine General Problem [12]. Consensus protocols are used in blockchain to reach a consistent state of the system where all or majority of the nodes accept the validity of the block even with some of the nodes in networks acting maliciously. Some of the most prominent consensus protocols include Proof-of-Work (PoW), Proof-of-Stake (PoS), Proof-of-Authority (PoA), etc. Some of the features provided by blockchain include Decentralization, Security, Transparency, Immutability, and Faster processing by removing centralized entities.

Evaluating E-Prescription System Against Blockchain. Even though blockchain provides many features, it cannot be a solution for every application. Hence each application has to satisfy certain conditions for applying blockchain [17].

Criteria: Does the current application need tamper-proof permanent storage?
Evaluation: E-prescription systems are intended to store the prescription information of the patients for enabling them to keep a record of their medication and to avoid adverse interactions of medications prescribed for other conditions. As this application needs permanent storage, blockchain can be a solution.

Criteria: Are there multiple trust-less data contributors to the data?
Evaluation: E-prescription systems consist of many distributed entities which include a network of prescribers, a network of patients, a network of pharmacies, and other regulating bodies. All these entities are distributed geographically and don't trust each other and need a co-coordinating central authority in order to relay. information. As there are multiple trustless data contributors in the network, blockchain can be a solution.

Criteria: Does the application modify data after storage?
Evaluation: Issuing prescriptions, and dispensing prescribed medicines generally don't need modifications once processed and prescribed medicines are dispensed to patients. If there are any mistakes in the prescription, a new prescription should be sent while invalidating the previous prescription. Hence, blockchain can be an acceptable solution in this case.

Criteria: Is data privacy required?
Evaluation: According to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) [7], sensitive patient information shouldn't be disclosed without the

patient's consent. Blockchain as such doesn't provide privacy on shared data as the data will be stored at multiple nodes in the network. But in the current application, we have used Cipher Text Policy - Attribute Based Encryption (CP-ABE) which will enable patients with full control over their prescription information and only encrypted data is being shared using off-chain storage Inter Planetary File System (IPFS).

Features of blockchain technology can provide an additional layer of security for the E-Prescription system by creating an immutable log of all transaction which help in maintaining the integrity of prescription data. Immutable log created acts as a single source of truth which is available at all the distributed participating entities and help to reduce prescription fraud. Blockchains also enhance interoperability by enabling different healthcare providers to participate and share data in the network transparently. As digital wallets are used for performing transactions on a blockchain network, the privacy of patients is maintained which will prevent data leakages.

3 Related Prior Works

Blockchain is one of the recent technological advancements which was introduced primarily for digital currency systems which enable P2P money transfers that are faster, and more reliable, and at any point in time digital assets will be under the control of the owner instead of centralized entities like banks. The features of blockchain including transparency, data integrity and security, working in a trust-less environment, and consensus-based updates have shown promising solutions in many other fields. Whether it is to store and manage Electronic Health Records [18,22] or secure medical supply chain [2,4–6] healthcare industry has been benefited largely by adapting blockchain technology. Different studies are conducted to build E-Prescription by leveraging blockchains. Comparison of proposed FortiRx with state-of-art is clearly shown in Table 1.

Table 1. Comparative Analysis of Proposed FortiRx with state-of-art.

	Blockchain Platform	**Smart Contracts**	**Off-chain storage**	**Data Privacy**	**Access Control Mechanism**	**CP-ABE**
Thatcher, et al. 2018 [20]	Ethereum	✓	✗	✗	✗	✗
Musamih, et al. 2021 [14]	Ethereum	✓	✓	✗	✓	✗
Taylor, et al. 2022 [19]	Ethereum	✓	✗	✓	✓	✗
Alnuaimi, et al. 2022 [3]	Ethereum	✓	✓	✗	✓	✗
Ionescu, et al. 2022 [11]	Ethereum	✓	✗	✗	✗	✗
FortiRx (Current Paper)	Ethereum	✓	✓	✓	✓	✓

A use case of blockchain as a Prescription Drug Monitoring System (PDMP) is presented in [20]. This proposed system leverages smart contracts on the Ethereum platform for the creation and management of prescriptions. Even though the proposed mechanism is providing a solution to manage E-Prescriptions, it mainly uses on-chain storage which could be very expensive for large amounts of information, and no access control mechanism is defined which will create a lot of security threats in the system. Another application of blockchains in prescription drug supply is given in [25]. This work provides a dynamic identity mechanism to prevent patient privacy issues along with a robust authentication protocol combined with blockchain. However, the proposed architecture doesn't deal with prescription management. Another blockchain-based solution for controlled medication is discussed in [14]. In this work, smart contracts and the Ethereum platform are used for building the controlled medicine prescription system along with using IPFS as off-chain storage. However, No access control mechanism is implemented in IPFS which will make data available for all the participants in the IPFS network.

VigilRx proposed in [19] makes use of smart contracts and the Ethereum platform to create a system for creating and managing prescriptions, it also implemented a robust access control mechanism using the RBAC mechanism. However, prescription information is stored on-chain which can be difficult to manage and is not cost-effective. Similar to previously proposed solutions, blockchain-based health insurance claims for prescription drugs are proposed in [3] which leverages the Ethereum blockchain and smart contracts. In this proposed architecture IPFS is used as a solution for storing prescription data to avoid on-chain overhead. Even though an efficient mechanism for managing insurance claims is proposed, Prescription information stored in IPFS is prone to data privacy risk as the information will be stored at all the participating public nodes in the IPFS network. Another implementation of the Ethereum platform and smart contracts can be seen in [11]. However, this proposed system doesn't address both data privacy concerns and the overhead costs of on-chain data storage.

4 Novel Contributions of the Current Paper

Below are problems with centralized E-Prescription systems which are addressed in the proposed FortiRx architecture along with novel solutions proposed.

4.1 Problems with Centralized E-Prescription System Addressed in FortiRx

Problems with existing centralized e-prescription systems which are addressed by novel proposed FortiRx architecture are:

- Centralized architecture in E-prescription systems can lead to a Single Point of Failure (SPOF).
- As the number of transactions increases, latency increases significantly.
- Lack of standardization can cause difficulty in integrating the systems with other Electronic Health Record Systems (EHR).
- Centralized systems are more prone to security threats and lead to other forms of fraud and prescription abuse.

- Cost of deployment and maintenance of E-prescribing systems is huge and makes it not accessible for all healthcare providers.
- Complexity of using such technology can also resist some people from adopting e-prescription systems.

4.2 Novel Solutions Proposed

The novel contributions of the proposed FortiRx are:

- Proposed FortiRx makes use of blockchain combined with the distributed file system (IPFS) to create a decentralized environment for all the participating entities to share prescription data.
- Blockchain creates a distributed trust-less environment to share data which enhances the interoperability of the system.
- Usage of distributed file-sharing system to store prescription information can help in reducing the amount of on-chain data.
- Due to the decentralized nature of the proposed FortiRx, It is resistant to Single Point of Failure (SPOF) and also reduces response latency.
- It avoids data tampering and prescription abuse by maintaining a distributed ledger that acts as a single source of truth.
- Proposed FortiRx also makes use of Cipher text-Policy attribute-based encryption (CP-ABE) to provide a robust access control mechanism.

5 Preliminaries of Cipher Text-Policy Attribute-Based Encryption (CP-ABE)

5.1 Bilinear Map

A bilinear map in CP-ABE are called pairings which associates pairs of elements from two groups G_1 and G_2 to a third group G_T. When G_1=G_2 the pairing is called symmetric otherwise asymmetric. Such a map function is denoted as $e : G_1 \times G_2 \rightarrow G_T$ and must satisfy the following properties:

- Bilinearity: For all $a, a' \in G_1$ and $b, b' \in G_2$, we have:

$$e(a + a', b) = e(a, b) \cdot e(a', b) \tag{1}$$

  and

$$e(a, b + b') = e(a, b) \cdot e(a, b') \tag{2}$$

- Non-degeneracy: There exist generators g_1 and g_2 of G_1 and G_2, respectively, such that $e(g_1, g_2)$ is a generator of G_T.
- Computability: The bilinear map function e can be efficiently computed.

Bilinear map is used in CP-ABE to compute pairing of two elements $g_1^a \in G_1$ and $g_2^b \in G_2$. This is done by using the equation:

$$e(g_1^a, g_2^b) = e(g_1, g_2)^{ab} \tag{3}$$

5.2 Setup

During setup, a trusted entity generates the system parameters which include the master secret key, a description of the bilinear map, and the groups used in the encryption and decryption process. A master secret key generated is used to generate the private keys for different attributes. Below are the steps followed in the setup function:

- Choose a Elliptic curve E and two cyclic groups G_1 and G_2 of order q such that $E(G_1, E_2) \subseteq G_T$.
- Choose corresponding generators g_1 and g_2 for two groups G_1 and G_2 respectively.
- Choose a master secret key randomly $a \in \mathbb{Z}_q$.
- Generate the set A = a * g2.
- publish the generated system parameters (E,G_1,G_2,G_T,e(g_1,g_2),A) and master secret key a is kept secret at the trusted entity.

5.3 Key Generation

A set of attributes are assigned to a user which is used to generate a private key for that user. The set of attributes associated with the user will be sent to the trusted entity which makes use of the master secret key along with the set of attributes to generate a decryption key.

5.4 Encryption

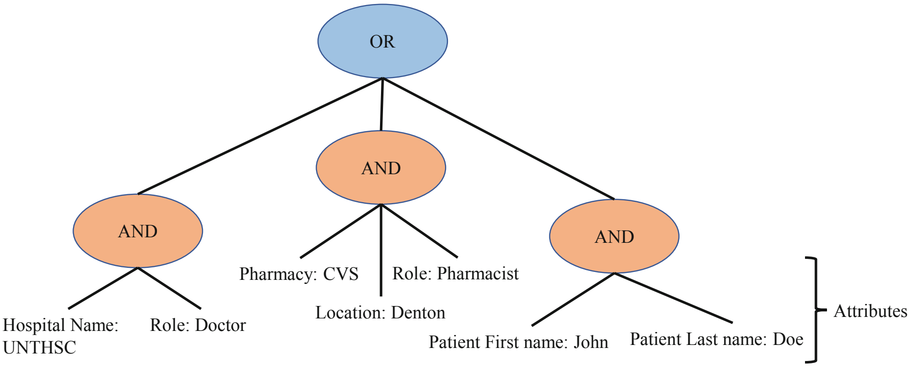
To encrypt a message using CP-ABE, the plain text message is first mapped to the elements in the encryption group. Next, a policy is defined using a set of attributes required to decrypt the cipher text. The defined policy is then mapped elements in the encryption group. After that plain text is then encrypted using the policy as an additional parameter to generate cipher text.

5.5 Decryption

A user with an appropriate set of attributes will first retrieve the decryption key and then uses the decryption key to decrypt the cipher text to plain text.

5.6 Access Policy

The access policy in CP-ABE is a logical expression defined using Boolean operators AND, OR, and NOT that specifies the attributes which are required to decrypt the ciphertext. Each set of attributes is associated with a secret key and all the cipher texts with access policy satisfying these attributes will be able to decrypt. A sample access policy is shown in Fig. 2.



Access Policy = ((“Hospital Name”== “UNTHSC” AND “Role”== “Doctor”) OR (“Pharmacy”==“CVS” AND “Location”==“Denton” AND “Role”==“Pharmacist”) OR (“Patient First Name”==“John” AND “Patient Last Name”==“Doe”))

Fig. 2. Sample Access Policy for Prescription.

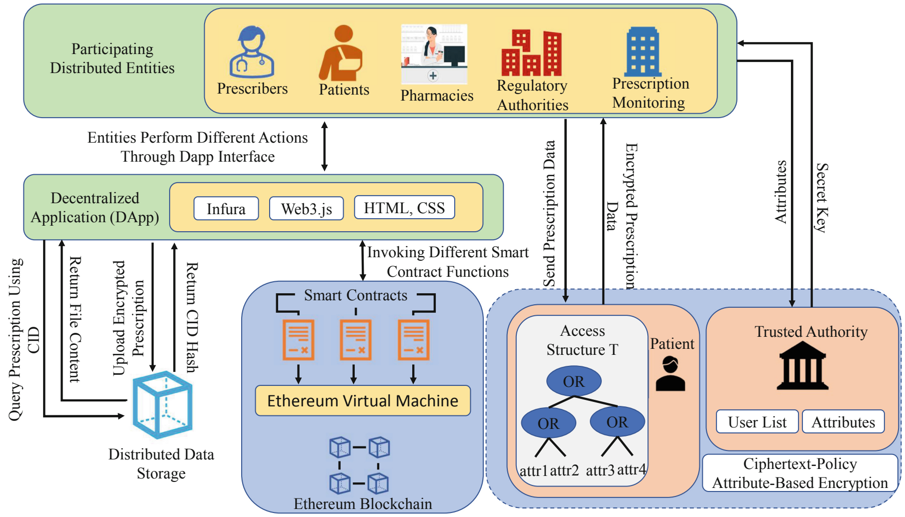


Fig. 3. Architectural Overview of Proposed FortiRx System.

6 Architectural Overview of the Proposed FortiRx

System level architecture view of the proposed FortiRx is shown in Fig. 3. Many distributed entities participate and share data in the proposed FortiRx which include prescribers, patients, pharmacies, Regulatory authorities, and in some cases authorities from prescription monitoring for controlled substance prescriptions. Prescriber is responsible for creating digital prescriptions information and encrypting them before sending the files to distributed data storage. Access Policy for encryption is provided by the patients that will determine who is allowed to access the data based on the issue attributed by a trusted authority.

One of the major problems with blockchain is managing large amounts of data on-chain which can be expensive too. Prescription systems generate large amounts of data within a short span of time and managing such data on-chain is not a viable solution. Hence, in the proposed FortiRx, we have used an off-chain distributed data storage solution to handle all the prescription information. Even though data is stored at all the decentralized nodes, implemented CP-ABE mechanism will make sure only the entities having properly assigned attributes defined in the access policy can decrypt it which ensures data privacy.

The proposed FortiRx architecture leverages smart contracts to implement business logic which include issuing the prescriptions, updating the status of prescription, requesting refills, approval for refills, and verifying the authenticity of prescription. Apart from business logic, a robust Role-based Access Control mechanism (RBAC) is also designed to ensure the entities can access only allowed functions. Every transaction by any of the entities participating will generate an event in the blockchain and will be added to the immutable log. Participating entities will access the functions of smart contracts through Decentralized Application (DApp) designed.

7 Proposed Algorithms for FortiRx

The prescription creation and uploading process is shown in Algorithm 1. After performing the diagnosis, an electronic prescription file will be generated with all the prescription information along with the patient information and dosages. This file will be read and the file content is encrypted by using the public parameters generated during the setup process of CP-ABE along with the access policy which will be decided by the patient. Once the encryption process is done, the generated cipher text will be written to a file and uploaded to the distributed data storage (IPFS). A content ID will be returned once the file upload is successful which is useful during the retrieval process. Prescriber usually the physician then creates a transaction using the patient's Ethereum address and content ID from IPFS to create a prescription entry in the blockchain. RBAC mechanism implemented in the smart contract will ensure the transaction is coming from the actual prescriber before updating the details of the patient account. Once the transaction is successful, the transaction hash and generated prescription ID will be sent back to the called and in case of any errors, the transaction will be discarded.

Retrieval of prescription data from IPFS and decryption is clearly explained in Algorithm 2. The Entity trying to access will make a function call to the smart contract using the prescription ID generated during the upload process. Based on the prescription ID, details of the prescription along with the IPFS hash are retrieved. This IPFS hash which is also the content ID will be used to request IPFS for retrieving the prescription content. Retrieved prescription content is an encrypted string and to decrypt it, the entity needs the secret key. The entity then sends its attributes to the trusted authority to get the secret key to decrypt the prescription content. If attributes satisfy the policy defined during the encryption, the content will be decoded and accessible to the requesting entity. If not, the content cannot be decrypted ensuring data privacy.

Algorithm 1 Proposed Prescription Upload Algorithm for FortiRx.

```
Input: Digital Prescription Data, public parameters $(params, g_1, g_2, e)$ generated during CP-ABE setup, Access policy $\rho$ defined by the patient
Output: Content ID for IPFS file, Transaction hash of prescription creation in blockchain
A digital prescription is generated, and a file is created
for Each prescription file f do
    Open file in read mode
    FileItem ← open(filePath,'r')
    Read prescription content from the file
    prescription content $(P_{content})$ ← fileItem.read()
    Encryption is done using public key (pk) and policy $\rho$ to generate ciphertext of the prescription content
    Cipher text $CT$ ← cpabe.encrypt(pk, $P_{content}$ ,$\rho$)
    New file is created and generated cipher text is written to that file
end for
for Each encrypted prescription file f do
    Send upload request to IPFS
    Response (res) ← requests.post(Infura end point, authentication parameters, file f)
    Content ID from response is retrieved
    Content ID (CID) ← res.text['Hash']
end for
Prescriber creates a new createPrescription transaction in prescription smart contract
Transaction $(Tx)$ ← prescription.createPrescription(patient address $(P_{addr})$,CID)
if caller == Prescriber then
    New prescription is created and added to patient address
    Emit an event (ev) with prescription data and a log is generated
    Return transaction hash $(Tx_{hash})$
else
    Reject $Tx$
end if
```

The status of the prescription is also updated once medicines are dispensed by the pharmacy. The pharmacy creates a transaction call to the prescription smart contract with the prescription id as the parameter. RBAC mechanism implemented will ensure the requesting Ethereum address is assigned a pharmacy role and it is one of the registered pharmacies for the patient. Similarly, in the case of refills, the pharmacy will update the status of the prescription requestRefill flag and notify the prescribers to approve. Different steps involved in this process are shown in Algorithm 3

8 Implementation of FortiRx

8.1 Smart Contract Design

We have used solidity language to design smart contracts and deployed them in the Ethereum platform. As there are multiple entities with each one having its own functions to perform, the access control mechanism is important. We have developed a Role

Algorithm 2 Proposed Prescription Retrieval Algorithm for FortiRx.

```
Input: Prescription ID ($P_{ID}$) generated while creating new prescription in blockchain, attribute
    list of requesting entity ($attr\_list$)
Output: Decrypted prescription content ($P_{content}$)
for Each view request ($req$) do
    Send a function call to prescription smart contract to retrieve Prescription based on $P_{ID}$
    Retrieved prescription $P_{ret}$ ← prescription.viewPrescription($P_{ID}$)
    Get IPFS Hash (CID) from the function response
    CID ← $P_{ret}$['IPFSHash']
    Send request to IPFS to retrieve prescription content ($P_{content}$)
    Response (res) ← requests.post(Infura end point, CID, authentication parameters)
    Retrieved cipher text ($CT$) ← res.text
    Secret key for set of attributes $attr\_list$ is requested from trusted authority
    Secret key ($Sk$) ← cpabe.keygen(public key (pk), $attr\_list$)
    Decrypt cipher text using the secret key to get prescription content
    if $\rho$.evaluate($attr\_list$) then
        $P_{content}$ ← cpabe.decrypt($Sk$, $CT$)
    else
        Cannot decrypt prescription content
    end if
end for
```

Based Access Control Mechanism (RBAC) using smart contract functions and modifiers. For each type of entity: Patient, Prescriber, and Pharmacy, three role smart contracts are defined which have different functions to add users to the role, check if the given address has been assigned with a role, and revoke the roles. Along with these modifiers are also defined to check for attaching them to the functions. Modifiers are used to impose some pre and post-conditional checks on the function parameters passed.

The main business functionality of prescription creation and management is done in "FortiRx.sol" smart contract which has two mappers which are used to keep track of prescriptions generated and another one to associate prescriptions to the patient's Ethereum address which will make it easy to retrieve. A function is developed for creating new prescriptions, this is restricted only to prescribers who are usually physicians. This creates new prescription functions and takes the patient address and Content ID of the prescription uploaded to IPFS as parameters. Another important function is the update prescription status function which is restricted to role of a pharmacy. Once the prescription is dispensed, the pharmacy will call this function to update the prescription to be filled and creates a log in the blockchain. In case of refill is required, the pharmacy can also make a call to function request refill which takes the prescription id as a parameter and updates the flag for a refill. On checking the flag, prescribe can approve the refill. A view function is also created to retrieve and view prescription details (Not the content of the prescription and patient information). Complete Class diagram of designed smart contracts for proposed FortiRx can be seen in Fig. 4.

Algorithm 3 Status Updates for Prescription on Blockchain.

```
Input: Prescription ID ($P_{ID}$) generated while creating new prescription in blockchain
Output: The Status of the prescription will be updated
Different status flag updates will be sent either by pharmacy or physician
Based on the type of status update, different functions of the smart contract will be invoked
  with ($P_{ID}$) as parameter
if Prescription is filled then
    prescription.updatePrescriptionStatus($P_{ID}$)
    Smart contract check the pharmacy Ethereum address for access and updates isFilled flag
      of prescription
else if Prescription needs re-filling then
    prescription.requestRefill($P_{ID}$)
    Smart contract checks the pharmacy Ethereum address for access and updates the
      requestRefill flag of prescription
else
    prescription.issueRefill($P_{ID}$)
    Smart contract checks the physician's Ethereum address for access and updates the isFilled
      and requestRefill flags of prescription
end if
```

8.2 Blockchain Network

The proposed FortiRx system is implemented using the Ethereum platform leveraging smart contracts designed in solidity language. A decentralized application (DApp) is designed using the truffle framework and a functionality test is performed using chai. Implemented FortiRx is first deployed in the local Ganache blockchain which mimics the working of Ethereum mainnet but provides 10 free accounts with test ether of 100 ETH each. For measuring performance analysis of the implemented system, it is then deployed in Ethereum testnet Sepolia. Sepolia is a permissioned Proof-of-Stake (PoS) consensus-based testnet. As it is a public testnet and hosts many other DApps with live transactions happening, evaluating FortiRx can give better results to evaluate reliability and adaptability in a real-world deployment scenario.

8.3 Distributed Data Source

Inter-Planetary File System (IPFS) is used for providing distributed data sources to store all the prescription information. As discussed before, storage is expensive and hard to manage on-chain. As the prescription application needs large amounts of information to be stored and retrieved, the off-chain distributed data storage solution IPFS is used. As it is impractical for all the users of blockchain to host their own nodes to participate in the network, we have used the infura platform which provides tools to connect to Ethereum easily and perform transactions. Infura also provides tools to connect to IPFS without hosting a node. IPFS connection uses the authentication parameters to authenticate the user before uploading the files.

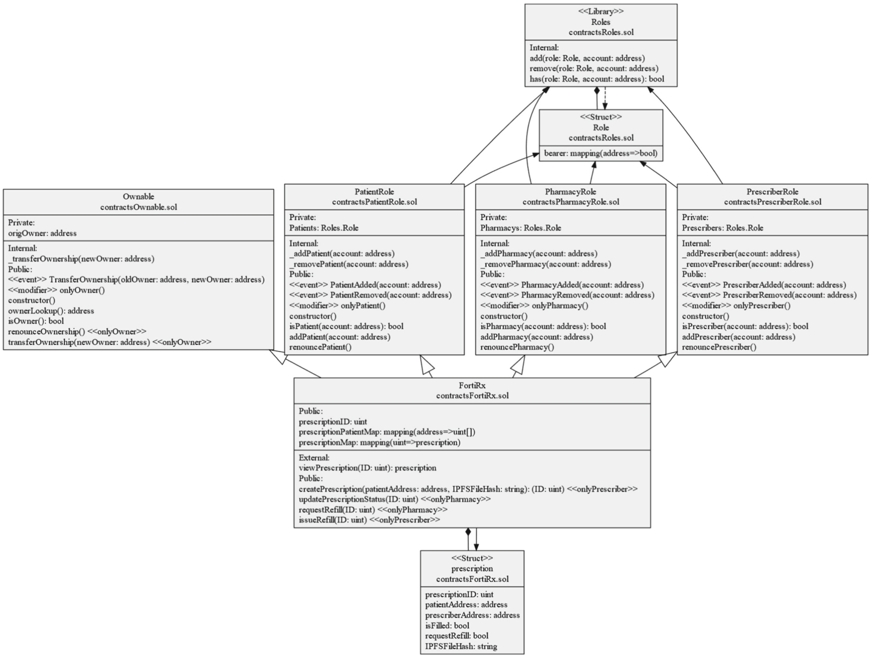

<<Library>>
Roles
contractsRoles.sol
Internal:
add(role: Role, account: address)
remove(role: Role, account: address)
has(role: Role, account: address): bool
<<Struct>>
Role
contractsRoles.sol
bearer: mapping(address=>bool)
Ownable
contractsOwnable.sol
Private:
origOwner: address
Internal:
_transferOwnership(newOwner: address)
Public:
<<event>> TransferOwnership(oldOwner: address, newOwner: address)
<<modifier>> onlyOwner()
constructor()
ownerLookup(): address
isOwner(): bool
renounceOwnership() <<onlyOwner>>
transferOwnership(newOwner: address) <<onlyOwner>>
PatientRole
contractsPatientRole.sol
Private:
Patients: Roles.Role
Internal:
_addPatient(account: address)
_removePatient(account: address)
Public:
<<event>> PatientAdded(account: address)
<<event>> PatientRemoved(account: address)
<<modifier>> onlyPatient()
constructor()
isPatient(account: address): bool
addPatient(account: address)
renouncePatient()
PharmacyRole
contractsPharmacyRole.sol
Private:
Pharmacys: Roles.Role
Internal:
_addPharmacy(account: address)
_removePharmacy(account: address)
Public:
<<event>> PharmacyAdded(account: address)
<<event>> PharmacyRemoved(account: address)
<<modifier>> onlyPharmacy()
constructor()
isPharmacy(account: address): bool
addPharmacy(account: address)
renouncePharmacy()
PrescriberRole
contractsPrescriberRole.sol
Private:
Prescribers: Roles.Role
Internal:
_addPrescriber(account: address)
_removePrescriber(account: address)
Public:
<<event>> PrescriberAdded(account: address)
<<event>> PrescriberRemoved(account: address)
<<modifier>> onlyPrescriber()
constructor()
isPrescriber(account: address): bool
addPrescriber(account: address)
renouncePrescriber()
FortiRx
contractsFortiRx.sol
Public:
prescriptionID: uint
prescriptionPatientMap: mapping(address=>uint[])
prescriptionMap: mapping(uint=>prescription)
External:
viewPrescription(ID: uint): prescription
Public:
createPrescription(patientAddress: address, IPFSFileHash: string): (ID: uint) <<onlyPrescriber>>
updatePrescriptionStatus(ID: uint) <<onlyPharmacy>>
requestRefill(ID: uint) <<onlyPharmacy>>
issueRefill(ID: uint) <<onlyPrescriber>>
<<Struct>>
prescription
contractsFortiRx.sol
prescriptionID: uint
patientAddress: address
prescriberAddress: address
isFilled: bool
requestRefill: bool
IPFSFileHash: string

Fig. 4. UML Diagram of Implemented FortiRx Role and Prescription Smart Contracts

Table 2. Role Assigned Accounts and Transaction Hashes on Sepolia Testnet

Feature	Value
Physician Account Address	0x3d352313f4f5561d0ffbfda205b52a3c3b70af35
Pharmacy Account Address	0x3D352313F4f5561D0fFBfda205B52A3c3b70af35
Patient Account Address	0x2a9884dfa7E6890FE8AA99FE2486c613C32b697a
Contract Deployment Hash	0x798d1f5ff49f9df09b9856db2646cebc2029d5cd2a45c5ef0c1b9acb9f217c6f
Prescription Content ID	Qme7Sq8gLmE875kE79QyWWFy9wqQ4yHnTEHMur511PrZfF
Prescription Creation Hash	0xda5bd0ce943325696e91bfe140bd8cdd60eafdca6f2a41b07221e499bfe7f1f7

8.4 CP-ABE System Design

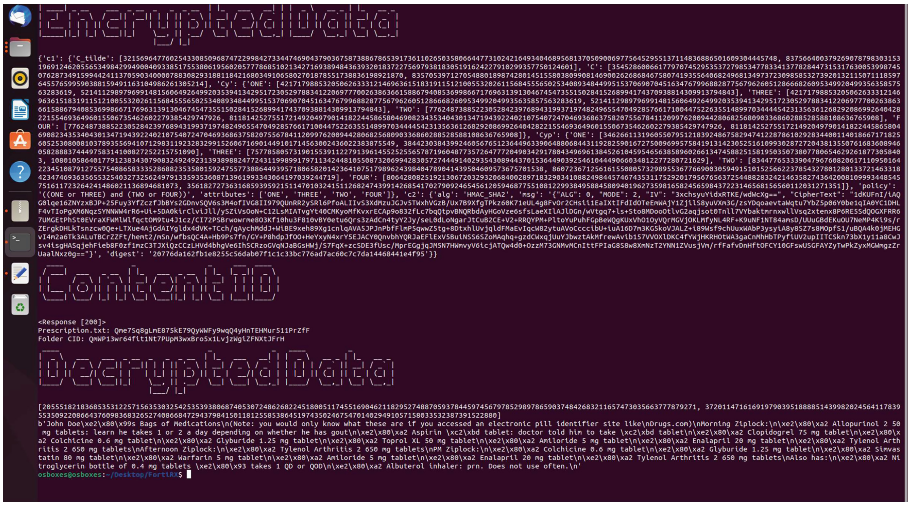
For implementing the CP-ABE scheme, Ubuntu 22.04 64-bit with a base memory of 4GB of memory is hosted in a virtual environment. For prototyping the proposed CP-ABE scheme for FortiRx, the charm crypto library is used. Charm is a framework that is designed to rapidly prototype cryptosystems and implement different schemes. GNU Multiple Precision Arithmetic Library (GMP), Pairing-Based Cryptography Library (PBC), and OpenSSL are prerequisites for installing the charm framework. CP-ABE scheme proposed in [23] is used for implementing FortiRx.

9 Experimental Results

This section discusses the results from the implemented proposed FortiRx application. Along with that security, timing, and cost analysis are also performed to evaluate the proposed system's reliability and adaptability.

9.1 Results

The first step of the proposed FortiRx application is creating a prescription text document. A sample electronic prescription is taken for testing purposes and is copied into a text file. The file is then encrypted using the CP-ABE scheme with a pre-defined access policy. Encrypted files are then uploaded to IPFS using infra. During the retrieval process, based on the CID the prescription data is retrieved and decrypted using a secret key generated from the attributes assigned to an entity. Encrypted prescription, Content ID, and Decryption of the prescription data can be seen in Fig. 5.



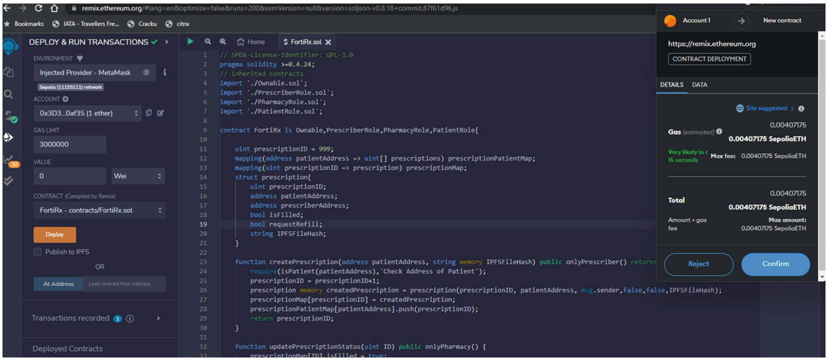
```
{'c1': {'C_tilde': [32156964776025433085096874722998427334474690437903675873886786539173611026503580664477310242164934046895681370509006977564529551371114836886501609304445748, 837566400379269078798303153
19691246205565349842994900409338517553806195602057778685102134271693894843639320183722756979381830519162422791029935775012460 1], 'C': [3545286006617797074529535372798534778334137782844731531763005399 8745
07628734915994424113705903400007883082931881184216803491065802701878551738836198921870, 835705397127054880189874280145155803809908146900262686846758074193556406824968134973723098585327392013211507111 8597
6455765995903881594911631049862613052 14], 'Cy': {'ONE': [42171798853205062633312146963615183191151210055320261156845556502534089348449951537069070451634767996882877567962605128666826095349920499356358575
63283619, 5214112989796991481560649264992035394134295172305297883412206977700263863661588679408536998667176963139130467454735515028415268994174370938814309913794843], 'THREE': [42171798853205062633312146
963615183191151210055320261156845556502534089348449951537069070451634767996882877567962605128666826095349920499356358575 63283619, 5214112989796991481560649264992035394134295172305297883412206977700263863
66158867940853699866717696313913046745473551502841526899417437093881430991379 4843], 'TWO': [776248738852230528423976894319937197482496554704928576617100447522635514899703444454231356361268292086992640428
2215546936496015506735462602279385429747926, 81181425275517214920497901418224458658046908234353404301347194392240210754072470469368637582075567841120997620094428068256809033686028852858810863676590 8], 'F
OUR': [7762487388522305284239768943199371974824965547049285766171004475226355148997034444542313563612682920869926404282215546936496015506735462602279385429747926, 8118142527551721492049790141822445865804
690823435340430134719439224021075407247046936863758207556784112099762009442806825680903368602885285881086367659 08]}, 'Cyp': {'ONE': [3462661131960550795121839248675829474122878610292834400114018667171825
605253080081037893556941071298311923283299152606716901449101714563002436022383875549, 38442303843992460567651236449633906488068443119282590167275009699575841913142305251610993028727204381355076168360 8946
05828883744497583141008272522157510 90], 'THREE': [757785805731901553911227913961455252556578719604877357264777204903429178043496961384526104595465638589602661347458825158195035073807780654629261877305840
3, 1080105864017791238343079083249249231393898824772431199899179711342448105508732069942830572744491402935430894437015364490392546104449066034812277280721629], 'TWO': [834477653339047967608206171109501 64
223451087912755754086583335286882353580159247557738864493957180658201423641075179896243984047890414395046095736757015 38, 8607236712561615508057329895536776690030594915101525662237854327801280133721463318
4234746936356553254032732562497913359353608713961993343064197039244719], 'FOUR': [80642808251921306720329320684002897183290341088249844574674353117529201795676563725448828324214635827436420081099934485 45
751611723264241486021136894681073, 35618272736316859395921511470103241511268247439914268541702790924654561205946877551081229938495884580940196273598165824565984372231465681565601120312713 51]}, 'policy':
'((ONE or THREE) and (TWO or FOUR))', 'attributes': ['ONE', 'THREE', 'TWO', 'FOUR']}, 'c2': {'alg': 'HMAC_SHA2', 'msg': '{"ALG": 0, "MODE": 2, "IV": "3xchsyuYidxRTKE/wdWcXg==", "CipherText": "1dKUFnI/iAQ
G0lqe16ZNYzxBJP+25Fuy3YfZczfJbBYs2GDnvSQV6s3M4ofIVG8II979QUnRR2ySRl6PfoALIIvS3XdMzuJGJv5TWxhVGzB/Ux7B9XfgTPkz60K71eUL4g8FvOr2CHsii1EaIXtIFdIdOTeEmWAjY1ZjilS8yuVXm3G/zsYDqoaevtaWqtu7YbZ5p06Y0be1qIA0YC1DHL
F4vTIoPgXM6NqzSYNNWW4rR6+Ui+5DA0kirClviJll/ySZiVsOoN+C12LsMIATvgYt40CMKyoMfKvxrECAp9o832fLc7bqQtpvBNQRbdAyHGoVze6sfsLaeXIlAJlDGn/wVtgq7+ls+Sto8MDooOtlvG2aqjsot0Tnll7VYbaktmrnxwllVsq2xtenx8P6RE5SdQOGXFRR6
7UMGEtPhSt0EVraXFWMlWlfqctOM9tu4J1cz/CI72PSBrwowrme8O3Kf10hu3F810vBY0etu6Qrs3zAdCn4tyY2Jy/seL0dLoNgarJtCuB2CE+V2+RRQYPM+PltoYuPuhFGpBeWQgKUxVhO1OyVQrMGVjOKLMfyNL4RF+K9uNF1NT84amsD/UUuGBdEKuOU7NeMP4Ki9s/r
ZErgkDHLkTsnzcw0Qe+LTXue4AjGdAIYgldx4dVK+TCch/qAychMddJ+WiBE9xeh89Xg1cnlqAVA5JPJnPbfFlmP5qwwZ5tg+8DtxhlUvjqldFMaEvIqcW82ytuAVoCcccibU+iuA16D7m3KG5koVJALZ+i89Wsf9chUuxWAbP3ysyiA8y8SZ7s8MOpfS1/uBQA4k0jMEHG
vI4m2a6Tk3ALuTBCrZZFt/hemt2/mSn/wfbsQC4A+Hb9Ps7fn/GY+P8hdpJfOO+HeYxyN4xrY5EJACY0QnvbhYQRJaEFlExV5BuiNSS6SZoMAqhq+gzdCWxqjUuYJbwztAkMfrewAvib157VVOXlDKC4fYWjHKRHOtWA3gaCnMhHbTPyfiUV2upIITCSkn73bX1y11a8CwJ
sv4isgHASqjehFieb8F0zf1mzC3TJXiQzCCzLHVd4bhgVe6IhSCRzoGVqNJaBGsHWj/S7FqX+zcSDE3fUsc/MprEGgjqJM5N7HWmvyV6icjATQw4d0+OzzM73GNMvMCnIttFPIaG8S8w8XmNzT2YNN1ZVusjVm/rfFafvDnHftOFCY10GFswUSGFAYZyTwPkZyxMGWmgzZr
UaalNxz0g=="}', 'digest': '20776da162fb1e8255c56dab07f1c1c33bc776ad7ac60c7c7da14468441e4f95'}}

<Response [200]>
Prescription.txt: Qme7Sq8gLmE875kE79QyWWFy9wqQ4yHnTEHMur511PrZfF
Folder CID: QmWP13wr64fit1Nt7PUpM3wxBro5x1LvjzWgiZFNXtJFrH

[2055518218368535312257156353032542535393806874053072486268224518005117455169046211829527488705937844597456797852989786590374842683211657473035663777879271, 3720114716169197903951888851439982024564117839
553509220866437609836832652740866847294379841501181255853864519743502467547014029491057158033532387391522880]
b'John Doe\xe2\x80\x99s Bags of Medications\n(Note: you would only know what these are if you accessed an electronic pill identifier site like\nDrugs.com)\nMorning Ziplock:\n\xe2\x80\xa2 Allopurinol 2 50
 mg tablets: learn he takes 1 or 2 a day depending on whether he has gout\n\xe2\x80\xa2 Aspirin \xc2\xbd tablet: doctor told him to take \xc2\xbd tablet\n\xe2\x80\xa2 Clopidogrel 75 mg tablet\n\xe2\x80\x
a2 Colchicine 0.6 mg tablet\n\xe2\x80\xa2 Glyburide 1.25 mg tablet\n\xe2\x80\xa2 Toprol XL 50 mg tablet\n\xe2\x80\xa2 Amiloride 5 mg tablet\n\xe2\x80\xa2 Enalapril 20 mg tablet\n\xe2\x80\xa2 Tylenol Arth
ritis 2 650 mg tablets\nAfternoon Ziplock:\n\xe2\x80\xa2 Tylenol Arthritis 2 650 mg tablets\nPM Ziplock:\n\xe2\x80\xa2 Colchicine 0.6 mg tablet\n\xe2\x80\xa2 Glyburide 1.25 mg tablet\n\xe2\x80\xa2 Simvas
tatin 80 mg tablet\n\xe2\x80\xa2 Warfarin 5 mg tablet\n\xe2\x80\xa2 Amiloride 5 mg tablet\n\xe2\x80\xa2 Enalapril 20 mg tablet\n\xe2\x80\xa2 Tylenol Arthritis 2 650 mg tablets\nAlso has:\n\xe2\x80\xa2 Ni
troglycerin bottle of 0.4 mg tablets \xe2\x80\x93 takes 1 QD or QOD\n\xe2\x80\xa2 Albuterol inhaler: prn. Does not use often.\n'
osboxes@osboxes:~/Desktop/FortiRX$
```

Fig. 5. FortiRx Implementation Showing Encrypted Prescription and Successful Upload to IPFS

Remix IDE is used to deploy smart contracts in sepolia testnet. MetaMask digital wallet is used for maintaining user accounts and sending transactions to Ethereum. Transaction for deploying the FortiRx contract is shown in Fig. 6. Once the contract is deployed Different accounts are assigned different roles: Prescriber (Physician), Pharmacy, and Patient accounts. Some of the important transactions and their corresponding addresses and hashes are shown in Table 2.



remix.ethereum.org/#lang=en&optimize=false&runs=200&evmVersion=null&version=soljson-v0.8.18+commit.87f61d96.js

DEPLOY & RUN TRANSACTIONS

ENVIRONMENT: Injected Provider - MetaMask (Sepolia (11155111) network)

ACCOUNT: 0x3D3...0af35 (1 ether)

GAS LIMIT: 3000000

VALUE: 0 Wei

CONTRACT (Compiled by Remix): FortiRx - contracts/FortiRx.sol

□ Publish to IPFS

Transactions recorded 1

Deployed Contracts

```
// SPDX-License-Identifier: GPL-3.0
pragma solidity >=0.4.24;
// inherited contracts
import './Ownable.sol';
import './PrescriberRole.sol';
import './PharmacyRole.sol';
import './PatientRole.sol';

contract FortiRx is Ownable,PrescriberRole,PharmacyRole,PatientRole{

    uint prescriptionID = 999;
    mapping(address patientAddress => uint[] prescriptions) prescriptionPatientMap;
    mapping(uint prescriptionID => prescription) prescriptionMap;
    struct prescription{
        uint prescriptionID;
        address patientAddress;
        address prescriberAddress;
        bool isFilled;
        bool requestRefill;
        string IPFSFileHash;
    }

    function createPrescription(address patientAddress, string memory IPFSFileHash) public onlyPrescriber() returns
        require(isPatient(patientAddress),'Check Address of Patient');
        prescriptionID = prescriptionID+1;
        prescription memory createdPrescription = prescription(prescriptionID, patientAddress, msg.sender,false,false,IPFSFileHash);
        prescriptionMap[prescriptionID] = createdPrescription;
        prescriptionPatientMap[patientAddress].push(prescriptionID);
        return prescriptionID;
    }

    function updatePrescriptionStatus(uint ID) public onlyPharmacy() {
        prescriptionMap[ID].isFilled = true;
```

Account 1 → New contract

https://remix.ethereum.org

CONTRACT DEPLOYMENT

Site suggested

Gas (estimated): 0.00407175 — 0.00407175 SepoliaETH

Very likely in < 15 seconds — Max fee: 0.00407175 SepoliaETH

Total: 0.00407175 — 0.00407175 SepoliaETH

Amount + gas fee — Max amount: 0.00407175 SepoliaETH

Fig. 6. Deployment of Smart Contract in Sepolia Testnet.

9.2 Validation

Security Analysis. Security analysis is performed on the proposed FortiRx to check the feasibility and adaptability of the system in real-world E-Prescription systems.
Threat 1: An adversary trying to gain access to sensitive information of patient
Solution: Proposed FortiRx makes use of a robust CP-ABE cryptography scheme. This will ensure the prescription data is only accessible to the authorized entities with assigned attributes and avoid data leakages. As blockchain uses identities based on the PKI system, anonymity is maintained while sending transacting in blockchain thereby preserving data privacy.
Threat 2: Fake transactions generated by an adversary in the blockchain network to introduce falsified information.
Solution: RBAC mechanism based on smart contracts and modifiers is defined in the proposed FortiRx which will ensure the functions are well-defined and given proper access to different entities. An adversary who will not have these privileges will not be able to send the transaction and create falsified information in the network.
Threat 3: Data manipulations by the adversary or prescription abuse by duplication.
Solution: Blockchain creates an immutable ledger with all the transactions generated from each and every participating entity. This ledger is copied at each node and acts as a single source of truth which is difficult to manipulate and easy to verify. This ensures no data modifications can be done to the data stored on the blockchain.

Timing and Cost Analysis. To perform timing and cost analysis, each smart contract interaction is repeated 10 times, and the average time taken for confirmation of transaction and gas cost is evaluated. Results from the analysis can be seen in Fig. 7 and Fig. 8. From timing analysis, it can be seen transaction times are not changed much based on the type of function as it mainly depends on the network congestion at the time of the transaction. So average delays ranging from 12–18 s is an acceptable delays in real-world applications. Cost analysis shows a significant difference between contract deployment and other functions as the cost depends on the number of instructions that need to be executed by the Ethereum Virtual Machine (EVM). The cost of deployment of a smart contract is 7.2$ converting ETH to US at the conversion rate of 1 ETH = 18000 USD whereas for all other functions is nearly a dime. The cost and latency can be avoided if private blockchain is implemented instead of using public blockchain.

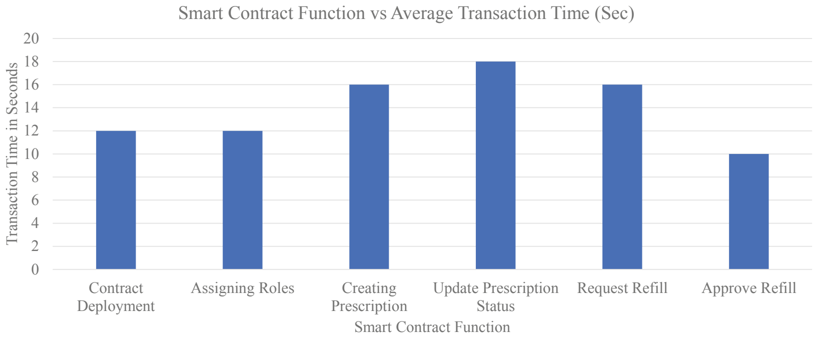


Fig. 7. Average Transaction Times of Smart Contract Functions.

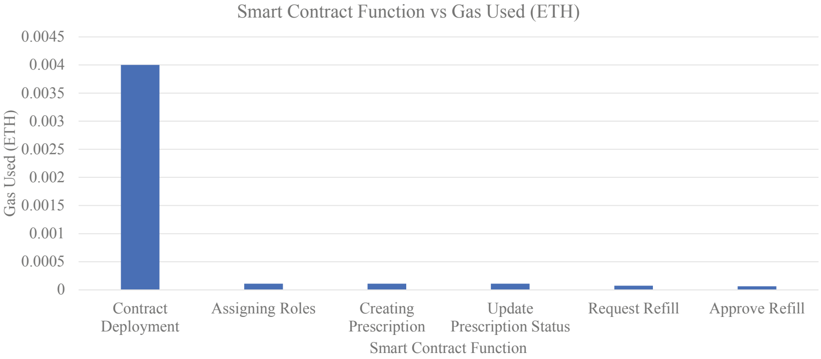


Fig. 8. Average Transaction Cost of Smart Contract Functions.

10 Conclusions and Future Research

In this work, we have proposed a novel idea of an E-Prescription system implemented using blockchain and smart contracts. The cost overhead of large on-chain data is addressed in the proposed FortiRx by implementing distributed data storage using IPFS. A robust access control mechanism using CP-ABE which ensures the efficient sharing of data between a dynamic group of data users has been implemented for preserving the privacy of patient information. This patient-centric approach will give more control to the data owners and efficiently manage the access mechanisms. Proof-of-Concept of proposed FortiRx is implemented and analyzed for scalability and reliability in real-world scenarios. Results from the analysis have shown the robustness of the proposed system for different security threats.

In future work, more scenarios and interactions will be included in the smart contract business logic to build a complete solution for the E-Prescription system. Implemented CP-ABE, even though provides a robust access control mechanism, it needs a centralized trusted entity to distribute attributes to the participants. A decentralized trustless key distribution mechanism can be beneficial in this case. Future work will be in the above scenarios along with providing a user-friendly interface for easy interaction with the system.

References

1. Ababneh, M.A., Al-Azzam, S.I., Alzoubi, K.H., Rababa'h, A.M.: Medication errors in outpatient pharmacies: comparison of an electronic and a paper-based prescription system. J. Pharmaceut. Health Serv. Res. **11**(3), 245–248 (2020). https://doi.org/10.1111/jphs.12356
2. Ahmadi, V., Benjelloun, S., Kik, M.E., Sharma, T., Chi, H., Zhou, W.: Drug governance: IoT-based blockchain implementation in the pharmaceutical supply chain. In: Proceedings of the Sixth International Conference on Mobile And Secure Services (MobiSecServ) (2020). https://doi.org/10.1109/mobisecserv48690.2020.9042950
3. Alnuaimi, A., Alshehhi, A., Salah, K., Jayaraman, R., Omar, I.A., Battah, A.: Blockchain-based processing of health insurance claims for prescription drugs. IEEE Access **10**, 118093–118107 (2022). https://doi.org/10.1109/access.2022.3219837
4. Bapatla, A.K., Mohanty, S.P., Kougianos, E., Puthal, D., Bapatla, A.: PharmaChain: a blockchain to ensure counterfeit-free pharmaceutical supply chain. IET Networks **12**(2), 53–76 (2022). https://doi.org/10.1049/ntw2.12041
5. Bapatla, A.K., Mohanty, S.P., Kougianos, E., Puthal, D.: PharmaChain 2.0: a blockchain framework for secure remote monitoring of drug environmental parameters in pharmaceutical cold supply chain. In: Proceedings of the IEEE International Symposium on Smart Electronic Systems (iSES) (2022). https://doi.org/10.1109/ises54909.2022.00046
6. Bapatla, A.K., Mohanty, S.P., Kougianos, E., Puthal, D.: PharmaChain 3.0: blockchain integrated efficient QR code mechanism for pharmaceutical supply chain. In: Proceedings of the OITS International Conference on Information Technology (OCIT) (2022). https://doi.org/10.1109/ocit56763.2022.00121
7. C for Disease Control (CDC). Health insurance portability and accountability act of 1996 (HIPAA). https://bitcoin.org/bitcoin.pdf. Accessed 18 Mar 2023
8. Food Administration. Working to reduce medication errors (2019). https://www.fda.gov/drugs/information-consumers-and-patients-drugs/working-reduce-medication-errors. Accessed 18 Mar 2023
9. Guo, H., Li, W., Nejad, M., Shen, C.C.: Access control for electronic health records with hybrid blockchain-edge architecture. In: Proceedings of the IEEE International Conference on Blockchain (Blockchain) (2019). https://doi.org/10.1109/blockchain.2019.00015
10. Huang, J., Qi, Y.W., Asghar, M.R., Meads, A., Tu, Y.C.: MedBloc: a blockchain-based secure EHR system for sharing and accessing medical data. In: Proceedings of the 18th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/13th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE) (2019). https://doi.org/10.1109/trustcom/bigdatase.2019.00085
11. Ionescu, S.V.: E-prescription using blockchain technology. In: Proceedings of the IEEE International Conference on Blockchain, Smart Healthcare and Emerging Technologies (SmartBlock4Health) (2022). https://doi.org/10.1109/smartblock4health56071.2022.10034520

12. Lamport, L., Shostak, R., Pease, M.: The byzantine generals problem. In: Concurrency: The Works of Leslie Lamport. Association for Computing Machinery (2019). https://doi.org/10.1145/3335772.3335936
13. Meyliana, S., Fernando, E., Cassandra, C., Marjuki: propose model blockchain technology based good manufacturing practice model of pharmacy industry in Indonesia. In: Proceedings of the 2nd International Conference on Innovative and Creative Information Technology (ICITech) (2021). https://doi.org/10.1109/icitech50181.2021.9590120
14. Musamih, A., Jayaraman, R., Salah, K., Hasan, H.R., Yaqoob, I., Al-Hammadi, Y.: Blockchain-based solution for the administration of controlled medication. IEEE Access **9**, 145397–145414 (2021). https://doi.org/10.1109/access.2021.3121545
15. Nakamoto, S.: Bitcoin: a peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf. Accessed 18 Mar 2023
16. World Health Organization. Medication without harm. https://www.who.int/initiatives/medication-without-harm. Accessed 18 Mar 2023
17. Puthal, D., Mohanty, S.P., Kougianos, E., Das, G.: When do we need the blockchain? IEEE Consum. Electron. Magaz. **10**(2), 53–56 (2021). https://doi.org/10.1109/mce.2020.3015606
18. Shahnaz, A., Qamar, U., Khalid, A.: Using blockchain for electronic health records. IEEE Access **7**, 147782–147795 (2019). https://doi.org/10.1109/access.2019.2946373
19. Taylor, A., Kugler, A., Marella, P.B., Dagher, G.G.: VigilRx: a scalable and interoperable prescription management system using blockchain. IEEE Access **10**, 25973–25986 (2022). https://doi.org/10.1109/access.2022.3156015
20. Thatcher, C., Acharya, S.: Pharmaceutical uses of blockchain technology. In: Proceedings of the IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS) (2018). https://doi.org/10.1109/ants.2018.8710154
21. Velo, G.P., Minuz, P.: Medication errors: prescribing faults and prescription errors. Br. J. Clin. Pharmacol. **67**(6), 624–628 (2009). https://doi.org/10.1111/j.1365-2125.2009.03425.x
22. Vora, J., et al.: BHEEM: a blockchain-based framework for securing electronic health records. In: Proceedings of the IEEE Globecom Workshops (GC Wkshps) (2018). https://doi.org/10.1109/glocomw.2018.8644088
23. Waters, B.: Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization. In: Catalano, D., Fazio, N., Gennaro, R., Nicolosi, A. (eds.) PKC 2011. LNCS, vol. 6571, pp. 53–70. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-19379-8_4
24. Wolf, M.S., Davis, T.C., Tilson, H.H., Bass, P.F., Parker, R.M.: Misunderstanding of prescription drug warning labels among patients with low literacy. Am. J. Health-Syst. Pharm. **63**(11), 1048–1055 (2006). https://doi.org/10.2146/ajhp050469
25. Ying, B., Sun, W., Mohsen, N.R., Nayak, A.: A secure blockchain-based prescription drug supply in health-care systems. In: Proceedings of the International Conference on Smart Applications, Communications and Networking (SmartNets) (2019). https://doi.org/10.1109/smartnets48225.2019.9069798
26. Zaghloul, E., Li, T., Ren, J.: Security and privacy of electronic health records: decentralized and hierarchical data sharing using smart contracts. In: Proceedings of the International Conference on Computing, Networking and Communications (ICNC) (2019). https://doi.org/10.1109/iccnc.2019.8685552

Survival: A Smart Way to Locate Help

Laavanya Rachakonda(✉) and Kylie Owen

Department of Computer Science, University of North Carolina, Wilmington, USA
{rachakondal,ko7529}@uncw.edu

Abstract. In 2020, nearly one hundred thousand deaths were drug related overdoses. In addition, forty to sixty percent of recovering addicts relapsed. A top contributor to relapsing is stress, as high levels of hormones are released within the brain. Individuals that could benefit from a rehabilitation center have many varied reasons as to why they do not seek one, proximity to a center being a primary reason. Rehabilitation facilities are a key factor in the recovery of an addict, as the probability of drug use decreases fifty to seventy percent after treatment. The hardest step in recovery is recognizing the need for help, however finding a treatment center can be a stressful experience, potentially leading to relapse. To reduce the stress of finding the closest and most qualified center, the goal of this research is to create a website that contains a database of rehabilitation centers. This could later be connected to a mobile application that would track the GPS location of the user and return the geographical location of the closest treatment center, as well as the name of the facility and contacting phone number. The software will have the ability to connect to wearable devices, allowing an opportunity to track physiological factors affected during an overdose.

Keywords: Smart Healthcare · Healthcare Cyber-Physical System (H-CPS) · Internet of Medical Things (IoMT) · Mental Health · IoT-Edge Computing

1 Introduction

Substance use disorder, or drug addiction is defined as the lack of control with the usage of substances. The definition of what drug addiction is can be enhanced as a cycle of decreased function of brain reward systems and recruitment of anti-reward systems that progressively worsen, resulting in the compulsive use of drugs [10]. Drug addiction can rewire the brains perceptions of 'rewards', making it more reliable on drugs due to the sense of euphoria experienced through the first couple of uses [6]. However, as the drug wears off, the body builds a tolerance to the drug of choice, and the euphoric sensations received from usage begin to lose their initial effect. This leaves users unsatisfied and in an opposing, aversive negative emotional state, contrasting the 'high' they sought initially [4].

2 Related Prior Research

A study was held to discover how anxiety affects an individual's chances of relapse [22]. Relapsing is defined as the return to drug-seeking and drug-taking behavior after

D. Puthal et al. (Eds.): IFIPIoT 2023, IFIP AICT 684, pp. 302–308, 2024.
https://doi.org/10.1007/978-3-031-45882-8_20

a prolonged period of abstinence [19]. It was determined that high levels of anxiety and stress often affect the ability of individuals to maintain abstinence from drug usage [18]. The study concluded that by understanding the relationship between anxiety and drug abstention from the perspective of emotions great significance for guiding individuals with substance use disorders in enhancing their drug abstention motivation by reducing negative emotion [21]. The patients with a better ability to maintain their own sense of self success, as well as positive emotions, are more likely to be able to balance how their anxiety affects the motivation they hold towards relapsing [22].

Stress is known to be a high contributor to a person's allostatic load, otherwise known as the negative effects of prolonged and chronic stress. An increased load results in progressive long-term changes in the brain. These chemical imbalances in the brain begin to weaken the strength of the parts that control emotions, thoughts, and actions while increasing the strength of the amygdala, affecting the individual's loss of control, cravings, and increased negative thoughts [17]. These changes create the opportunity for an individual to become more susceptible to drug cravings, and increased negative thoughts, all of which can lead to relapsing [21].

A study also tested what factors an individual may face that increases the odds of a relapse. The current age, age when the individual began using drugs, type of drug, and smoking habits all affect the chances of relapsing [2]. As the age of addicts increases, the chances of relapse increase respectively. However, individuals that began using drugs later in their life are less likely to relapse after undergoing rehabilitation services. The choice of drugs, in regards to modern versus traditional drugs, can affect the chances of relapsing, with modern drugs holding higher odds [8].

Oftentimes, relapse takes place after an individual has visited a rehabilitation center [7]. Rehabilitation is portrayed as the fix-all for substance use disorder, especially with the decreasing focus on justice in governmental elements. Though the biggest determining factors of the success of rehabilitation is support and provided treatment, the National Rehabilitation Implementation Committee clarifies that it is unlikely that any single agency can provide everything that is needed to address the issues contained within cycle of addition [3]. This concept of well-rounded rehabilitation can feel overwhelming and stressful, especially for those receiving the treatment. If this stress is added to pre-existing chemical imbalances within the brain, chances of relapse are higher if there is a lack pushing factors to justify the amount of effort needed to overcome the cycle of substance abuse [14].

A study was conducted to determine how the amygdala reacts to a drug relapse. The subjects were placed under different factors when the drug was being administered. Results from the study contain evidence showing that environmental factors were one of the most noticeable characteristics to trigger a relapse [21]. This concept shows that things, such as particular locations, specific light, etc. that are similar to that of the environment the euphoria from the drug was experienced, can elicit cravings that lead to a higher likelihood of a relapse. Different drugs have unique uses and euphoric experiences; however, many have similar characteristics, including physiological and mental effects. Some of the most commonly abused drugs are amphetamines, marijuana, opioids, cocaine, and phencyclidine [13].

Both modern and traditional drugs cause changes within the brain. Amphetamines heighten the central nervous system by increasing the number of neurotransmitters, such as dopamine, norepinephrine, and serotonin. Similarly, opioids increase the amount of dopamine released after connecting to the opioid receptors to block signals of pain [1]. Cocaine blocks the release of gamma-aminobutyric acids or GABA, an inhibitory neurotransmitter responsible for reabsorbing dopamine within the brain. Similarly, to the effects of cocaine use, phencyclidine prevents the absorption of dopamine, norepinephrine, and serotonin. Phencyclidine also blocks the NMDA receptors, preventing the production of glutamine known for affecting emotions, sensations of pain, learning, and memory of an individual. These changes within the brain can overwhelm chemical pathways and receptors, resulting in the brain attempting to limit these changes, affecting the body's tolerance to the drug, as previously mentioned [20].

3 Impact of Drugs on Mental Health

Drug usage in general can cause increased blood pressure and pulse rates, insomnia, loss of appetite, physical exhaustion, dilated pupils, and hyperactivity [5]. Symptoms of overdose can include increased body temperature, agitation, hallucinations, and convulsions. Withdrawal symptoms can include anxiety, fatigue, irritability, headaches, paranoia, depression, and body twitches [15].

Substance use among those struggling with post-traumatic stress disorder can often stem from the belief that the euphoria experienced will bring relief to symptoms experienced from the disorder. Post-traumatic stress disorder, also known as PTSD, is often seen to be tied with an imbalance of certain chemicals within the brain that are meant to help manage the stress levels of an individual. Without the correct presence of these stress-managing chemicals, individuals with PTSD can find themselves experiencing extreme levels of stress they have not experienced before, pushing them to find ways to balance the strain their conditions have placed on them [16]. The authors of Drug and Alcohol Dependence state that the increased severity and number of symptoms spawning from the presence of PTSD often fall hand-in-hand with the likelihood of substance abuse [12].

Almost seven percent of individuals struggle with post-traumatic stress disorder. People struggling with PTSD are fourteen times more likely to develop substance use disorder, or addiction. The continued use of substance can lead to increased anxiety and inability to be able to cope with trauma in a 'normal' way. Both substance abuse and PTSD are often found to be 'comorbid' [12]. Within the different types of drugs, the brain and mind of the individual is altered in a way that could allow them to become more susceptible to disorders, especially PTSD Though the euphoria of the first few usages of substances seem to bring relief to the symptoms of PTSD, consistent use of drugs produces the opposite effect than what was originally sought. Extended usage, in actuality, increases stress levels and symptoms that could both lead to PTSD or enhance pre-existing symptoms if the disorder is already present [9].

A study was held to determine the ties between PTSD and opioid dependency. Through this study it is shown that the patients who face drug dependency often face symptoms of PTSD when determined through the clinical criteria such the Maudsley

Addiction Profile, the Severity of Dependence Scale, the Impact of Events Scale, and the ICD-10 [9]. Over 30% of those involved in the study met the criteria qualifying them for diagnosis of post-traumatic stress disorder [9]. Within the four categories of the symptoms of PTSD, patients involved in the study had clinically significant levels of intrusive and avoidant symptoms; both of which majorly affect how an individual's quality of life is socially and emotionally, furthering the idea that PTSD can increase an individual's dependency on drug use.

4 Current Solution and Proposed Solution

As mentioned in Sect. 2, there are not many mechanisms to help patients or potential patients. Current practices show that the patients looking for rehabilitation services may experience relapse because of the additional stress [19]. Keeping this mind, Survival, a one stop destination to locate rehabs is proposed as shown in Fig. 1. This website has two interactive maps. One containing a database of hundreds of rehabilitation and counseling centers along with addresses and contact information across North Carolina as shown in Fig. 2. Another map containing the number of centers within each state across America as shown in Fig. 3 is proposed [11].

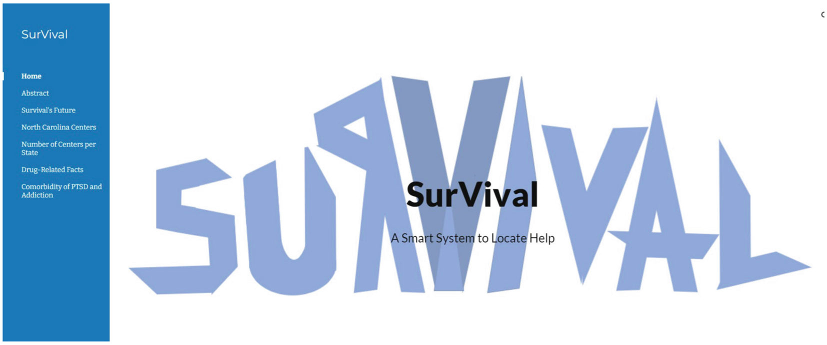


Fig. 1. Homepage of Survival.

The product of this research is meant to be straightforward and aware of the characteristics of substance use disorder, to help utilize technology for both those suffering from addiction and those interested in awareness as shown in Fig. 4. From the overarching theme of blue within the website, which studies have shown is the most calming color, to the use of interactive maps and the inclusion of the research's sources, Survival strives to be a low stress application, as stress is known to be a primary contributing factor of relapse [12]. The project's intention is to help in the recovery process when an individual wants assistance.

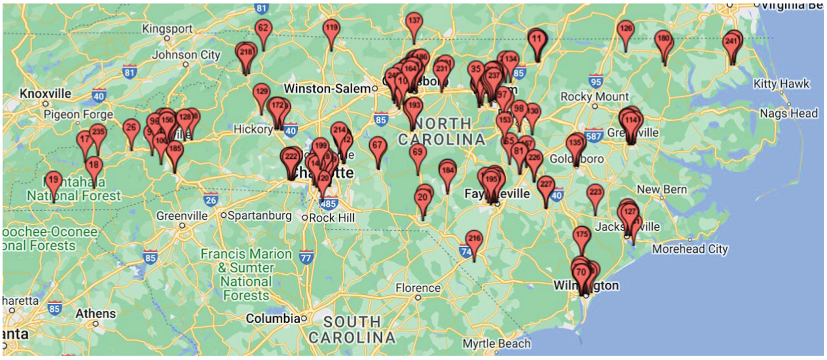
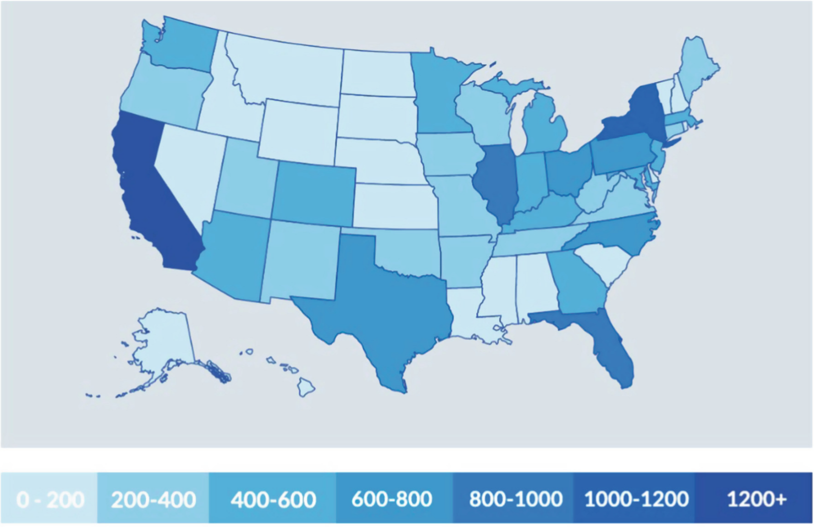
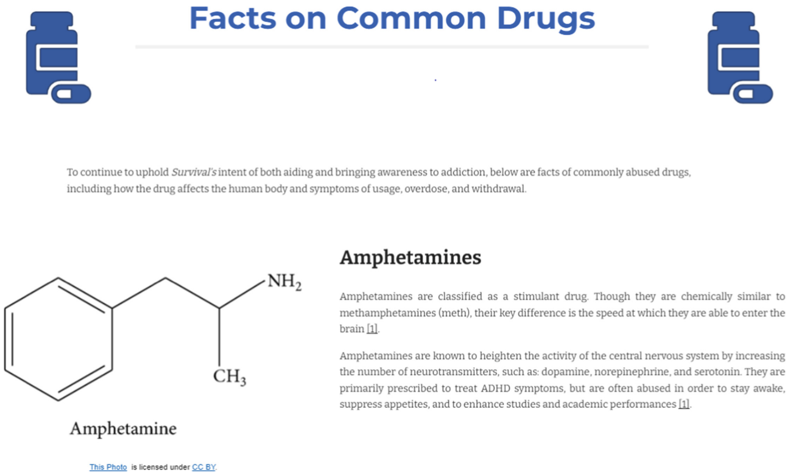


Fig. 2. Map view of the Rehabilitation Centers in North Carolina.



The key is in respect to the number of counseling and rehabilitation centers per state.

Fig. 3. Rehabilitation Centers across United States of America.



Facts on Common Drugs

To continue to uphold *Survival's* intent of both aiding and bringing awareness to addiction, below are facts of commonly abused drugs, including how the drug affects the human body and symptoms of usage, overdose, and withdrawal.

Amphetamine

This Photo is licensed under CC BY

Amphetamines

Amphetamines are classified as a stimulant drug. Though they are chemically similar to methamphetamines (meth), their key difference is the speed at which they are able to enter the brain [1].

Amphetamines are known to heighten the activity of the central nervous system by increasing the number of neurotransmitters, such as: dopamine, norepinephrine, and serotonin. They are primarily prescribed to treat ADHD symptoms, but are often abused in order to stay awake, suppress appetites, and to enhance studies and academic performances [1].

Fig. 4. Information on Drugs.

5 Conclusions and Future Research

Survival can be expanded further by being compatible with wearable devices, allowing an opportunity to track the physiological factors that are affected during an overdose. This will help to minimize the number of drug-related deaths by offering those struggling with addiction an opportunity to easily contact a facility. As addiction and post-traumatic stress disorder are known to be co-morbid, the intentions of the program could also advance to offering help geared towards individuals with PTSD.

Survival's usefulness could be furthered by developing a larger database containing a map of facilities across North Carolina across to include centers across the United States and worldwide. This would impact society for the better by offering a more accessible and straightforward way to find the centers meant to help in recovery, as well as bring attention to areas that lack facilities locations.

References

1. Administration, D.E.: Drug Fact Sheet: Marijuana/Cannabis (2020). https://www.dea.gov/sites/default/files/2020-06/Marijuana-Cannabis-2020.pdf
2. Amirabadizadeh, A., Nakhaee, S., Ghasemi, S., Benito, M., Torbati, V.B., Mehrpour, O.: Evaluating drug use relapse event rate and its associated factors using Poisson model. J. Subst. Use **26**(1), 60–66 (2021). https://doi.org/10.1080/14659891.2020.1779359
3. American Addiction Centers. Rehab Success Rates and Statistics (2022). https://americanaddictioncenters.org/rehab-guide/success-rates-and-statistics
4. American Addiction Centers. Barriers to Addiction Treatment: Why Addicts Don't Seek Help (2023). https://americanaddictioncenters.org/rehab-guide/treatment-barriers
5. BrightView Clinic. How do amphetamines affect the body. (2022). https://www.brightviewhealth.com/latest-updates/how-do-amphetamines-affect-the-body/

6. Center for Disease Control and Prevention. U.S. Overdose Deaths in 2021 Increased Half as Much as in 2020 - But Are Still Up 15 2023. https://www.cdc.gov/nchs/pressroom/nchs_press_releases/2022/202205.htm
7. Doyle, J., Ivanovic, J.: HSE national drug rehabilitation framework document. Tech. rep., Health Service Executive (HSE), pp. 1–38 (2010)
8. Drug Enforcement Administration. Drug Fact Sheet: Marijuana/Cannabis. Tech. rep., Drug Administration (2020). https://www.dea.gov/sites/default/files/2020-06/Marijuana-Cannabis-2020.pdf
9. Elman, I., Borsook, D.: The failing cascade: comorbid post traumatic stress and opioid use disorders. Neurosci. Biobehav. Rev. **103**, 374–383 (2019). https://doi.org/10.1016/j.neubiorev.2019.04.023
10. Koob, G.F., Moal, L.: Michel: addiction and the brain antireward system. Annu. Rev. Psychol. **59**(1), 29–53 (2008). https://doi.org/10.1146/annurev.psych.59.103006.093548. PMID: 18154498
11. Owen, K.: SurVival: A Smart System to Locate Help (2023). https://sites.google.com/view/survival-system-to-locate-help
12. National Center for PTSD. Understanding PTSD and PTSD Treatment. Techreport, US Department of Veterans Affairs (2019). https://permanent.fdlp.gov/gpo123944/understandingptsd_booklet.pdf
13. National Institute on Drug Abuse. Cannabis (Marijuana) Research Report: What are marijuana's effects? Tech. rep., National Institute on Drug Abuse (2020). https://nida.nih.gov/publications/research-reports/marijuana/what-are-marijuana-effects
14. National Institute on Drugs. Drugs, Brains, and Behavior: The Science of Addiction. National Institute on Drug Abuse (2020)
15. Patel, A., Bey, T.: Phencyclidine intoxication and adverse effects: a clinical and pharmacological review of an illicit drug. California J. Emerg. Med. **8**(1), 9–14 (2007)
16. Rachakonda, L., Bipin, K.C.: Tr-estimate: a novel machine learning based early prediction system for post-traumatic stress disorder using IoMT. In: IEEE International Symposium on Smart Electronic Systems (iSES), pp. 677–682 (2022). https://doi.org/10.1109/iSES54909.2022.00151
17. Rachakonda, L., Mohanty, S.P., Kougianos, E.: iLog: an intelligent device for automatic food intake monitoring and stress detection in the IoMT. IEEE Trans. Consum. Electron. **66**(2), 115–124 (2020). https://doi.org/10.1109/TCE.2020.2976006
18. Rachakonda, L., Mohanty, S.P., Kougianos, E., Sundaravadivel, P.: Stress-lysis: a DNN-integrated edge device for stress level detection in the IoMT. IEEE Trans. Consum. Electron. **65**(4), 474–483 (2019). https://doi.org/10.1109/TCE.2019.2940472
19. Ronald, E., Fuchs, R., Ledford, C., McLaughlin, J.: Drug addiction, relapse, and the amygdala. Annal. N. Y. Acad. Sci. **985**(1), 294–307 (2003). https://doi.org/10.1111/j.1749-6632.2003.tb07089.x
20. Ruisoto, P., Contador, I.: The role of stress in drug addiction. an integrative review. Physiol. Behav. **202**, 62–68 (2019). https://doi.org/10.1016/j.physbeh.2019.01.022
21. Ruisoto, P., Contador, I.: The role of stress in drug addiction, an integrative review. Physiol. Behav. **202**, 62–68 (2019)
22. Li, Y., Zeng, X., Zhou, H.: Relationship between anxiety and drug abstention motivation in men with substance use disorders: a cross-sectional study of compulsory isolation rehabilitation in China. J. Ethnicity Subst. Abuse **22**(1), 189–212 (2023). https://doi.org/10.1080/15332640.2021.1923103, PMID: 34543152

Federated Edge-Cloud Framework for Heart Disease Risk Prediction Using Blockchain

Uttam Ghosh[1], Debashis Das[2(✉)], Pushpita Chatterjee[3], and Nadine Shillingford[1]

[1] Department of CS and DS, Meharry Medical College, Nashville, TN, USA
ghosh.uttam@ieee.org, nshillingford@mmc.edu

[2] Department of CSE, Narula Institute of Technology, Kolkata, West Bengal, India
debashis.das@ieee.org

[3] Department of EE and CS, Howard University, Washington, DC, USA
pushpita.c@ieee.org

Abstract. Heart disease is a term used to describe a range of conditions that affect the heart, such as coronary artery disease, heart failure, and arrhythmias. It is a leading cause of death globally and can be prevented or managed through lifestyle changes and medical treatments, such as medication and surgery. The use of federated learning and edge computing has become increasingly popular for machine learning tasks, especially in the healthcare domain. However, privacy and security concerns remain major challenges in the adoption of such technologies. In this article, we propose a blockchain-enabled federated edge-cloud framework for heart disease risk prediction to address these challenges. The proposed framework involves the use of blockchain to secure the data sharing and model aggregation process, while edge devices are utilized for data preprocessing and feature extraction, and cloud servers are used for model training and validation. The federated learning approach ensures data privacy, while the use of blockchain provides immutability, transparency, and accountability to the system.

Keywords: Heart disease risk prediction · Federated learning · Blockchain · Healthcare · Edge computing · Privacy

1 Introduction

Heart disease is a major global health issue and a leading cause of death worldwide [27]. According to the World Health Organization (WHO), an estimated 17.9 million people die each year from cardiovascular diseases, which include heart disease [31]. Early detection and prevention of heart disease are crucial in reducing the impact of this disease. Heart disease risk prediction is important because it can help identify individuals who are at high risk of developing heart disease allowing for preventative measures to be taken. These measures can

Published by Springer Nature Switzerland AG 2024
D. Puthal et al. (Eds.): IFIPIoT 2023, IFIP AICT 684, pp. 309–329, 2024.
https://doi.org/10.1007/978-3-031-45882-8_21

include lifestyle changes such as diet and exercise as well as medical interventions such as medications or surgery. By identifying high-risk individuals early on, the likelihood of developing heart disease can be reduced to improved health outcomes and a reduction in mortality rates. With the advancement of technology, there is an opportunity to develop new approaches for heart disease risk prediction. One such approach is the use of a federated edge-cloud framework [1], which combines edge and cloud computing to process patient data in real time. However, existing approaches to heart disease risk prediction are often limited by data privacy and security issues as well as performance limitations (Fig. 1.).

Machine learning (ML) techniques have shown promise in predicting the risk of heart disease based on various clinical and non-clinical factors [23]. However, the use of ML in healthcare requires the integration of heterogeneous data sources, which are often distributed across different organizations and locations. One of the main challenges in heart disease risk prediction is the collection and processing of patient data. Current approaches often require large amounts of data to be collected and analyzed, which can be time-consuming and resource-intensive. The use of cloud-based solutions can also raise concerns about data privacy and security, as patient data is often transmitted over public networks. Federated learning (FL) [7] has emerged as a promising technique to address the challenges of collaborative and distributed ML.

To address these challenges, a Federated Edge-Cloud Framework for Heart Disease Risk Prediction (FECHD-RP) using Blockchain has been proposed. The FECHD-RP framework offers a promising solution to the challenges facing current approaches to heart disease risk prediction. By combining edge and cloud computing with blockchain technology [10], this system offers improved data privacy and security, as well as real-time data processing capabilities. This article provides a detailed technical introduction to this system, highlighting its

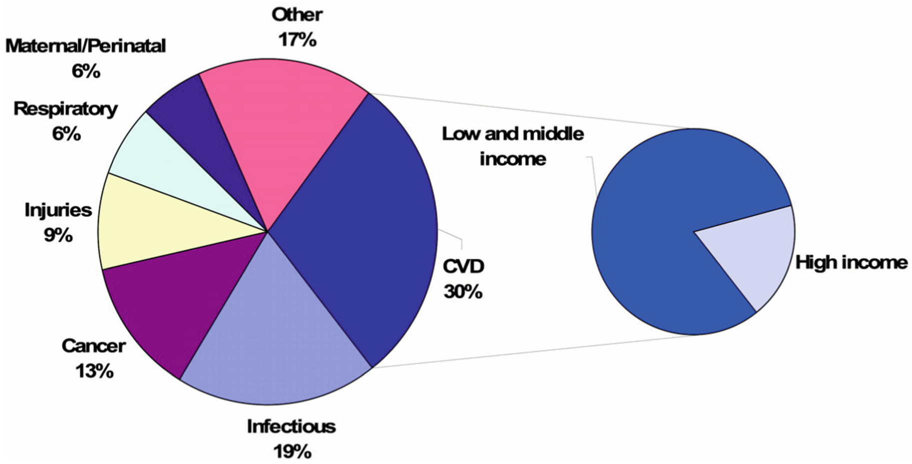


Fig. 1. Heart disease compared with other causes of death

potential to improve heart disease risk prediction and prevention. The use of a blockchain ensures the privacy and security of patient data [9], giving patients greater control over their own health data.

1.1 Motivation

COVID-19 has highlighted healthcare disparities for African Americans. Heart Failure (HF) is a costly and morbid illness, expected to impact 6.2 million people in the US, costing $30.7 billion and projected to reach $69.8 billion by 2030 [35]. A National Institutes of Health-supported study found racial disparities in advanced heart failure treatment, with non-African American adults twice as likely to receive mechanical heart pumps or transplants [5].

For health risk prediction, tracking calorie intake can be beneficial, as research shows it aids weight loss and sustains better overall health. Calorie counter apps and self-monitoring technologies offer helpful tools to keep track of dietary decisions [32]. Regarding cloud security in healthcare [14], common worries include information privacy, data security, availability, integrity, and network security. Problems with cloud computing involve doubts about security and privacy, slow organizations, loss of data governance, and lax safety standards. In some cases, service agreements lack clauses for clients to freely audit and control their data [29].

Existing issues with cloud-based health data include data security, visibility, management, misconfiguration, unauthorized access, and cyberattacks [25]. Ransomware poses a significant risk to data security in and outside the healthcare industry [8]. Therefore, safeguarding the security, availability, integrity, and privacy of health data is crucial, with users responsible for handling data appropriately, fostering trust with healthcare providers, and adhering to strict privacy and regulatory standards.

1.2 Contribution of the Paper

The main contribution of the article is the proposal of the FECHD-RP framework for heart disease risk prediction, which addresses privacy and security concerns while having the benefits of federated learning and edge computing in the healthcare domain.

- The paper introduces the concept of heart disease, its various forms, and its significance as a leading global cause of death. It highlights the potential for prevention and management through lifestyle changes and medical treatments.
- This paper discusses the growing popularity of federated learning and edge computing in the healthcare domain. It acknowledges the privacy and security concerns associated with these technologies, which hinder their widespread adoption.

- This paper presents the proposed solution: FECHD-RP framework for heart disease risk prediction, named FECHD-RP. The framework aims to address the privacy and security challenges by incorporating blockchain for secure data sharing and model aggregation. It outlines the specific components and roles within the proposed framework. It mentions the use of edge devices for data preprocessing and feature extraction, cloud servers for model training and validation, and blockchain for ensuring data security and accountability.
- The paper emphasizes the benefits of the federated learning approach, which protects data privacy by keeping the data distributed across devices while still allowing for collaborative model training. It highlights the advantages of blockchain in the proposed framework, including immutability, transparency, and accountability. These properties enhance the overall security and trustworthiness of the system.

1.3 Organization of the Paper

The remaining part of this paper is organized as follows. Section 2 depicts existing works on heart disease risk prediction using several methods by several researchers. In Sect. 3, several types of methods are discussed for heart disease risk prediction. Section 4 presents a proposed framework and discusses this work. Future works related to the proposed framework are given in Sect. 5. Finally, Sect. 6 concludes the paper.

2 Literature Review

A literature review on heart disease risk prediction demonstrates the significance of machine learning algorithms, genetic markers, and clinical parameters in accurately assessing an individual's risk (see Table 1). These approaches enhance early detection and aid in preventive measures, ultimately reducing cardiovascular disease prevalence. In order to solve the issues of training latency, communication cost, and privacy concerns in the biological data acquired by healthcare providers for the purpose of heart disease prediction, Yaqoob et al. [36] devised a hybrid architecture. For optimum feature selection and classification of heart disease, the client end of the framework makes use of a modified artificial bee colony optimization with a support vector machine (MABC-SVM). On the other hand, the HSP server makes use of federated matched averaging in order to circumvent problems with privacy. The results of the experiments reveal that the suggested method is superior to conventional federated learning strategies in terms of accuracy in prediction and classification, as well as the number of iterations required to achieve maximum precision.

Hasanova et al. [16] presented a machine learning-based Sine Cosine Weighted K-Nearest Neighbour (SCA_WKNN) algorithm for the prediction of heart illness. This algorithm acquires its knowledge from data that is kept on a blockchain that is resistant to tampering and is used for the safekeeping of patient information. The accuracy, precision, recall, F-score, and root mean square error of the

Table 1. Existing Heart Disease Prediction Model

Ref.	Approach	Key Findings	Limitations	Solutions
Yaqoob et al. [36]	Hybrid Framework	Improved prediction accuracy, reduced error	Training latency, communication cost, and privacy concerns	Modified artificial bee colony optimization with support vector machine (MABC-SVM) for feature selection and classification of heart disease, and federated matched averaging to overcome privacy issues
Hasanova et al. [16]	Machine Learning	The Sine Cosine Weighted K-Nearest Neighbour algorithm outperforms other algorithms in terms of accuracy	Lack of secure storage for patient information	Machine learning based Sine Cosine Weighted K-Nearest Neighbour (SCA_WKNN) algorithm for heart disease prediction using tamper-resistant blockchain for secure storage of patient information
Yuan et al. [37]	Machine Learning	Excellent accuracy and stability in binary and multiple classification predictions	Data complexity and overfitting	Fuzzy logic and gradient boosting decision tree (GBDT) for reducing data complexity and increasing generalization of binary classification prediction; Bagging to avoid overfitting for multiclassification prediction
Khan et al. [19]	IoMT Framework	Accuracy of 99.45% with precision of 96.54%	Search capability and learning parameters optimization	Modified salp swarm optimization (MSSO) using Levy flight algorithm for improving search capability; Adaptive neuro-fuzzy inference system (ANFIS) learning parameters optimization using MSSO to prevent getting trapped in local minima
Aarmah et al. [30]	IoT and Deep Learning	High-level security with an accuracy of 95.87%	Data transmission security	Wearable IoT device data encryption using the PDH-AES technique for secure data transmission; Deep Learning Modified Neural Network (DLMNN) for heart disease classification
Mohan et al. [22]	Machine Learning	The accuracy level of 88.7% with hybrid random forest with a linear model (HRFLM)	Feature selection and classification techniques	Hybrid random forest with a linear model (HRFLM) for feature selection and classification
Nashif et al. [26]	Cloud-based System	Accuracy level of 97.53%, sensitivity of 97.50%, and specificity of 94.94%	Real-time patient monitoring	Cloud-based heart disease prediction system using machine learning techniques; Real-time patient monitoring system using Arduino for continuous supervision of heart disease patients

proposed method are compared to those of existing algorithms. According to the findings, SCA_WKNN performs better than other algorithms when it comes to accuracy. In addition, peer-to-peer storage and blockchain-based decentralized storage are compared with regard to latency and throughput, with blockchain-based decentralized storage reaching a better throughput.

Yuan et al. [37] developed a heart disease prediction model that was based on machine learning and could simultaneously accomplish binary and multiple classifications. The Fuzzy-GBDT approach is the outcome of the model's combination of fuzzy logic and the gradient boosting decision tree (GBDT) [11], which aims to both minimize the amount of complexity in the data and raise the generalization of binary classification prediction. The Bagging-Fuzzy-GBDT is developed by the combination of the Fuzzy-GBDT and bags in order to prevent overfitting. The findings of the evaluation demonstrate that the Bagging-Fuzzy-GBDT model has superior accuracy as well as stability in binary as well as multiple classification predictions.

The major focus of Khan et al.'s [19] research was on developing an IoMT framework for the prediction of cardiac illness by using modified salp swarm optimization (MSSO) and an adaptive neuro-fuzzy inference system (ANFIS) [6]. MSSO enhances the search capabilities by using the Levy flight algorithm, and it also optimizes the learning parameters of ANFIS to avoid it from being mired in local minima. Both of these features may be found in MSSO. MSSO-ANFIS is used to categorize sensor data from medical records, such as blood pressure, age, sex, chest pain, cholesterol, and blood sugar, in order to diagnose the heart problem. Other factors that may be considered include cholesterol and blood sugar levels. According to the findings of the simulations, the suggested MSSO-ANFIS prediction model achieves an accuracy of 99.45% with a precision of 96.54%, which is a greater level of performance than that of previous methods.

Sarmah et al. [30] suggested study provides a patient monitoring system that makes use of deep learning and the internet of things in order to diagnose heart disease (HD). Steps for authentication and encryption are included in the system, which ensures the confidentiality of data transfer. The PDH-AES encryption method [30] is used to encrypt the sensor data before it is sent from the wearable Internet of Things device and then decoded in the cloud. After the data has been encrypted, it is put through a Deep Learning Modified Neural Network (DLMNN) [24], which determines if the cardiac conditions are normal or pathological. If the results were abnormal, the doctor would be notified immediately so that they could begin treatment. The PDH-AES method that has been developed offers a high degree of security, with an accuracy of 95.87% and a short amount of time required for encryption and decryption respectively. The findings of the experiments indicate that the DLMNN classifier works better than other algorithms currently used for HD diagnosis.

Mohan et al. [22] used machine learning to find significant variables to improve cardiovascular disease prediction. When utilized with the proposed prediction model, which uses many feature combinations and classification procedures, the hybrid random forest with a linear model (HRFLM) [23] achieves

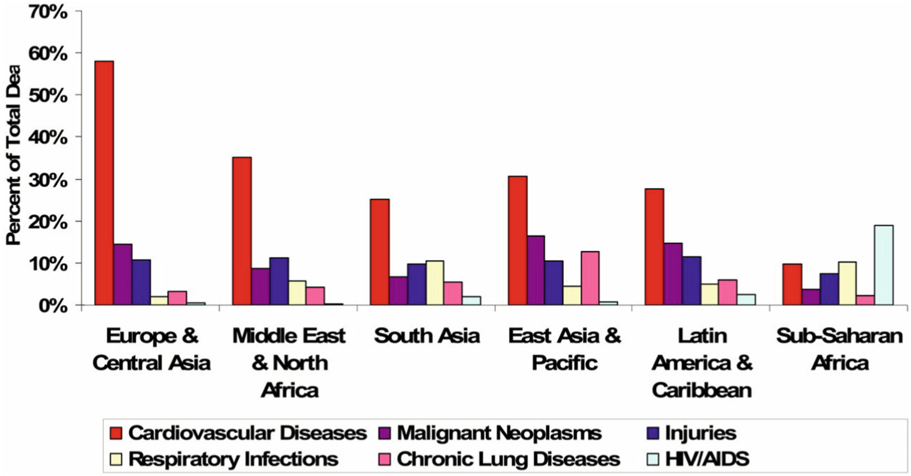


Fig. 2. Major causes of death in persons of all ages

88.7% accuracy. This article discusses how machine learning may be used in the Internet of Things (IoT) [9] and in healthcare to make predictions and judgments.

Nashif et al. [26] created a cloud-based heart disease prediction system using machine learning. Two prominent open-access databases tested the proposed method. Its accuracy, sensitivity, and specificity were 97.53%, 97.50%, and 94.94%, respectively, using the SVM method [33]. Arduino created a real-time patient monitoring system. This system can sense a patient's body temperature, blood pressure, humidity, and heartbeat in real time, transmit the data to a central server, and notify the doctor via GSM if any parameter exceeds the threshold. Body temperature, blood pressure, humidity, and pulse are other real-time characteristics. Physicians may use an app to see real-time sensor data and transmit live video for emergency treatment. This monitors heart disease patients continuously.

3 Heart Disease Risk Prediction

The process of determining an individual's chance of acquiring cardiovascular disease (CVD), which encompasses disorders such as coronary artery disease, heart failure, and stroke, is referred to as heart disease risk prediction. Models used to estimate the risk of cardiovascular disease often take into account a number of risk variables, including age, gender, history of the illness in the family, smoking status, blood pressure, cholesterol levels, diabetes, and obesity. These risk variables are analyzed by the models, which then calculate an individual's probability of acquiring cardiovascular disease within a certain amount of time, such as 10 years. The findings of a heart disease risk prediction may be used to assist therapeutic decision-making. For example, they might be used to determine if a patient would benefit from making changes to their lifestyle, taking drugs, or participating in other treatments to lower their chance of developing CVD.

3.1 Existing Methods

Several risk prediction models exist, including the Framingham Risk Score, the Reynolds Risk Score, and the QRISK Score. These models have been validated in different populations and have varying levels of accuracy, so healthcare providers must select the appropriate model for their patient population and interpret the results with caution. Several heart disease risk prediction methods are proposed by several researchers, as shown in Table 2. Some of these are presented below:

Framingham Risk Score. The Framingham Risk Score is a widely used tool to estimate an individual's risk of developing cardiovascular disease, including heart disease. The score is calculated using a combination of risk factors such as age, gender, blood pressure, cholesterol levels, and smoking status. It provides an estimate of an individual's risk over a 10-year period and helps identify those who may benefit from early interventions, such as lifestyle modifications and medication. However, it has limitations in predicting risk for certain populations, such as those with diabetes, and does not account for all potential risk factors. Despite its limitations, the Framingham Risk Score remains a valuable tool for estimating heart disease risk and guiding preventative measures.

QRISK3. QRISK3 is a tool used to estimate an individual's risk of developing cardiovascular disease, including heart disease. It takes into account a wide range of risk factors, including age, gender, ethnicity, smoking status, blood pressure, cholesterol levels, body mass index, and family history of heart disease. QRISK3 also accounts for additional risk factors such as medical conditions and socioeconomic status, which the Framingham Risk Score does not. QRISK3 provides a 10-year estimate of an individual's risk and can guide interventions to reduce that risk. It has been found to be more accurate than previous versions of the tool and can help identify individuals who may benefit from early preventative measures.

ASCVD Risk Estimator. An individual's risk of developing atherosclerotic cardiovascular disease (ASCVD), which includes heart disease and stroke, may be determined with the use of a tool called the ASCVD Risk Estimator. It takes into consideration potential danger variables such as age, gender, whether or not a person smokes, blood pressure, cholesterol levels, and whether or not they have diabetes. An individual's 10-year risk of getting ASCVD may be estimated using the calculator, which can also be used to assist guide measures aimed at reducing that risk. Its primary use is in clinical settings, and both the American College of Cardiology and the American Heart Association endorse its utilization when attempting to determine the likelihood of developing ASCVD. However, it does have a few drawbacks, such as the fact that it does not take into consideration some risk variables and that its accuracy suffers in certain groups.

Reynolds Risk Score. An individual's risk of acquiring cardiovascular diseases, such as heart disease and stroke, may be estimated with the use of a tool called the Reynolds Risk Score. Traditional risk variables including age, gender, blood pressure, cholesterol levels, and smoking status are taken into consideration, in addition to additional risk factors such as a family history of cardiovascular disease and C-reactive protein levels. The Reynolds Risk Score offers a 10-year estimate of a person's risk and is largely used in clinical settings to suggest measures that lower that risk. The score also provides an individual with an overall risk score. Traditional risk scores, which do not take into consideration levels of C-reactive protein, have been proven to be less accurate than this method, which has been found to be more accurate. On the other hand, it has certain shortcomings in terms of estimating risk for particular groups and may not be suitable for everyone.

SCORE. Systematic Coronary Risk Evaluation, often known as SCORE, is a method that was created by the European Society of Cardiology to quantify an individual's risk of acquiring cardiovascular disease, which may include heart disease and stroke. Traditional risk variables including age, gender, blood pressure, cholesterol levels, and smoking status are all taken into consideration. The SCORE tool gives an assessment of an individual's risk over a 10-year period in addition to providing distinct estimates for low-risk and high-risk locations in Europe. Its primary use is in clinical settings, where it is used to direct interventional efforts aimed at lowering that risk. However, it does have a few drawbacks, such as the fact that it does not take into consideration all of the possible risk variables and that its accuracy suffers in some groups. Because of this, it has to be used in combination with clinical judgment and elements that are unique to the patient.

DeepHeart. DeepHeart is an algorithm for deep learning that was developed by researchers at the University of California, San Francisco. These risk factors include age, sex, blood pressure, and smoking status. It is intended to be a technology that may detect persons at risk of developing cardiovascular disease in a way that is inexpensive and does not include any intrusive procedures. The algorithm has shown encouraging results in predicting risk variables, and it has the potential to enhance screening and diagnosis of cardiovascular disease in a way that is both efficient and cost-effective. However, further study is required to verify its accuracy and demonstrate its value in clinical settings.

EHR-Based Models. Electronic Health Record (EHR)-based models are tools that make use of patient data that is maintained in electronic health records to make predictions about an individual's risk of acquiring a variety of health issues, including cardiovascular disease. These models take into account an extensive variety of patient data, such as demographic information, medical history, laboratory values, medication usage, and diagnostic procedures. These data are analyzed using a variety of methods including logistic regression, machine learning, and artificial neural networks using models that are based on EHRs. The results of this analysis are estimations of an individual's risk. These models have the potential to increase the accuracy of risk prediction and identify people who might potentially benefit from early treatments. However, they do have certain limitations, such as problems with data quality, bias, and concerns around privacy. Before putting them into clinical use, it is necessary, as a result, to demonstrate both their precision and their dependability.

Wearable Devices. Wearable devices are portable electronic devices that may be worn on the body, such as smartwatches and fitness trackers. These devices are outfitted with sensors to collect and send data relating to physical activity, heart rate, sleep, and other health parameters. Examples of wearable devices include fitness trackers and smartwatches. These devices offer the ability to enable continuous monitoring of a person's health state in real-time, including the risk that an individual may acquire cardiovascular disease. Changes in patterns of physical activity, heart rate, and other vital indicators may be monitored by sensors that can be worn on the body. These changes may indicate an increased risk of cardiovascular disease. They also have the ability to give feedback and encouragement to improve lifestyle behaviors like physical exercise, food, and sleep, all of which may help minimize the chance of developing cardiovascular disease. However, there are also worries over the accuracy and dependability of wearable devices, as well as their potential to generate anxiety or overdiagnosis. These issues are related to the potential of the gadgets. For this reason, it is essential to confirm the accuracy and dependability of these devices and to interpret the data within the context of the individual's overall health state.

Genetic Risk Scores. Genetic risk scores are a kind of instrument that may evaluate an individual's likelihood of acquiring a variety of health issues, including cardiovascular disease, by making use of that individual's genetic information. These scores are derived by conducting an analysis of genetic differences known as single nucleotide polymorphisms (SNPs), which are linked to an elevated probability of acquiring the disorder. Scores for genetic risk may be determined using a variety of methods, such as polygenic risk scores, which assess total genetic risk by combining data from several SNPs. These scores may help offer an estimate of an individual's lifetime risk of getting a disease and can also assist in guiding preventative measures or screening programs. However, genetic risk scores have certain drawbacks, including the fact that they do not take into account environmental or lifestyle variables that may contribute to illness risk and the possibility that they are not relevant to all populations. For this reason, genetic risk scores should be used in combination with clinical assessments and other risk variables in order to offer a thorough evaluation of an individual's potential for developing cardiovascular disease.

Biomarkers. Biomarkers are quantifiable indications of biological processes that take place inside the body. These indicators may be used to diagnose illness or keep an eye on its progression. Biomarkers may be used in the context of cardiovascular disease to identify people who are at an elevated risk of acquiring the condition, as well as to monitor the development of the disease and response to therapy. Blood lipids (such as cholesterol and triglycerides), high-sensitivity C-reactive protein (hs-CRP), natriuretic peptides (such as B-type natriuretic peptide or NT-proBNP), and cardiac troponins are some frequent biomarkers used in cardiovascular disease. Other biomarkers include high-sensitivity C-reactive protein (hs-CRP). These biomarkers may be used to assist identify people who may benefit from preventative treatments, as well as to help guide treatment choices and monitor a patient's response to therapy. However, there are a number of drawbacks associated with the use of biomarkers, including their variable results, lack of specificity, and expense. Therefore, in order to offer a thorough evaluation of an individual's risk of developing or treating cardiovascular disease, they should be utilized along with other clinical examinations and risk factors.

Coronary Artery Calcium Scoring. The coronary artery calcium score is a non-invasive imaging test that utilizes computed tomography (CT) to assess the amount of calcium accumulation in the coronary arteries. This buildup, which may be a symptom of atherosclerosis and an elevated risk of cardiovascular disease, can be scored using the coronary artery calcium score. A low-dose CT scan of the heart is performed during the test, and then specialized software is used to determine a calcium score based on the quantity and density of calcium deposits found in the coronary arteries of the patient. After obtaining this score, an individual's likelihood of acquiring cardiovascular disease may be calculated using this score. The calcium scoring of the coronary arteries has been found to be a valuable technique for risk assessment, especially in persons who are considered to be at an intermediate risk, and it may assist guide preventative activities as well as treatment choices. However, there are several drawbacks to the test, including the possibility of being exposed to ionizing radiation and the possibility of receiving false-positive findings, both of which might result in unneeded measures. Therefore, in order to offer a thorough evaluation of an individual's risk of developing or treating cardiovascular disease, it should be utilized in combination with other clinical examinations and risk factors.

Machine Learning Models Using Imaging Data. Machine learning models using imaging data are tools that use artificial intelligence algorithms to analyze medical images, such as computed tomography (CT) scans, magnetic resonance imaging (MRI) scans, and echocardiograms, to identify patterns and make predictions about an individual's risk of developing cardiovascular disease. These models use large datasets of medical images and associated clinical data to train algorithms to recognize patterns and associations that are difficult for humans to detect. Machine learning models can provide more accurate and precise risk prediction, aid in the diagnosis of cardiovascular disease, and help guide treatment decisions. However, they have limitations such as requiring large datasets for training, the need for high-quality imaging, and potential biases in the data. Therefore, it is important to validate the accuracy and reliability of these models and interpret the data in the context of the individual's overall health status.

Digital Phenotyping. Digital phenotyping refers to the use of digital data, such as smartphone data, social media data, and wearable device data, to assess an individual's behavior, mood, and cognitive function. In the context of cardiovascular disease, digital phenotyping can be used to track physical activity levels, sleep patterns, and other lifestyle behaviors that may contribute to the development or progression of cardiovascular disease. It can also be used to assess stress levels, mood, and other psychosocial factors that may impact cardiovascular health. Digital phenotyping has the potential to provide a more comprehensive and real-time assessment of an individual's health status, allowing for more personalized and timely interventions. However, there are also concerns about privacy, data security, and the accuracy and reliability of the data. Therefore, it is important to ensure that digital phenotyping tools are validated and used in an ethical and responsible manner to ensure the protection of an individual's privacy and rights.

Lifestyle Factors. It involves evaluating an individual's lifestyle habits and behaviors to estimate their risk of developing cardiovascular disease. Lifestyle factors that are commonly considered in risk assessment include smoking status, physical activity levels, dietary habits, alcohol consumption, and stress levels. These factors can have a significant impact on an individual's risk of developing cardiovascular disease, and interventions targeting these factors can help reduce the risk. Lifestyle-based risk assessment can be used to identify individuals who may benefit from lifestyle modifications, such as improving dietary habits, reducing stress, and quitting smoking. However, lifestyle factors are often interrelated, and individual factors may interact with each other to impact overall risk. Therefore, a lifestyle-based risk assessment should be used in conjunction with other clinical assessments and risk factors to provide a comprehensive evaluation of an individual's risk of developing or managing cardiovascular disease.

Hybrid Models. Hybrid cardiovascular disease risk assessment models use various risk variables and prediction algorithms to produce a more accurate risk estimate. For example, a hybrid model may incorporate both traditional risk factors, such as age, sex, blood pressure, and cholesterol levels, as well as non-traditional risk factors, such as biomarkers, genetic risk scores, or imaging data. Machine learning algorithms may also be used to integrate and analyze these different types of data to identify patterns and associations that may not be apparent using traditional statistical models. Hybrid models have the potential to provide a more personalized and precise estimate of an individual's risk of developing cardiovascular disease and can help guide preventive interventions and treatment decisions. However, they are also more complex and may require more resources for implementation and validation compared to simpler risk assessment models. Therefore, hybrid models should be carefully evaluated and validated to ensure their accuracy and reliability.

4 Proposed Framework

The FECHD-RP framework comprises three main components: edge devices, a cloud server, and a federated learning coordinator. The edge devices are responsible for collecting and processing patient data, including medical records, lifestyle factors, and environmental factors. The edge devices also perform the initial training of the ML models using the local data. The cloud server provides additional computing resources and storage to support the federated learning process. The federated learning coordinator is responsible for coordinating the training of the ML models across edge devices and cloud servers, ensuring data privacy and security. However, each component is described below:

Edge Devices. Edge devices are any computing devices that are located on the periphery of the network, such as smartphones, wearables, or IoT devices. In the context of the FECHD-RP framework, edge devices collect medical data

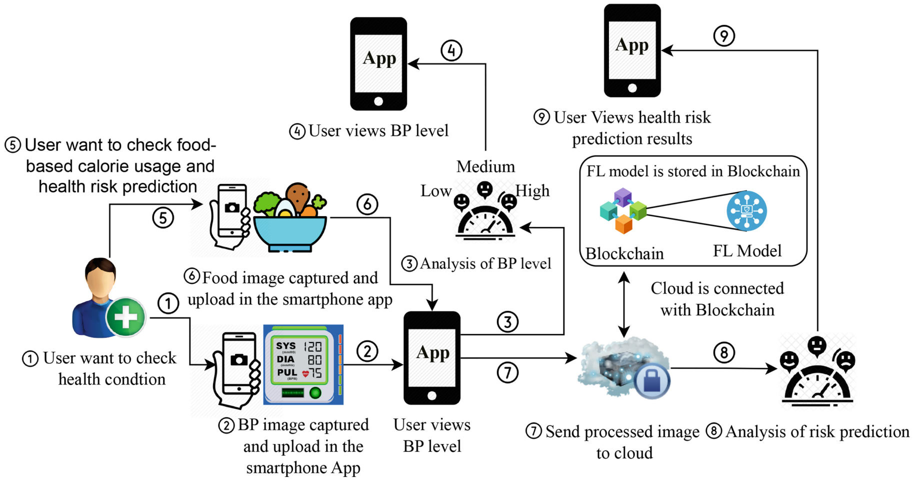

App
④
④ User views BP level
App
⑨
⑨ User Views health risk prediction results
⑤ User want to check food-based calorie usage and health risk prediction
⑤
⑥
Medium
Low
High
③ Analysis of BP level
FL model is stored in Blockchain
Blockchain
FL Model
Cloud is connected with Blockchain
⑥ Food image captured and upload in the smartphone app
①
① User want to check health condtion
SYS 120
DIA 80
PUL 75
②
App
③
⑦
⑧
② BP image captured and upload in the smartphone App
User views BP level
⑦ Send processed image to cloud
⑧ Analysis of risk prediction

Fig. 3. Proposed framework.

such as heart rate, blood pressure, and other health-related data from patients. These devices then use a local machine learning model to analyze this data and make predictions about a patient's risk of heart disease. The predictions made by each edge device are then shared with the cloud server for further analysis.

Cloud Server. The cloud server plays a crucial role in the proposed framework for heart disease risk prediction. Beyond aggregating and analyzing data from edge devices, it serves as the central hub for collaborative model training and validation through federated learning. This approach allows the cloud server to leverage the collective knowledge from multiple edge devices while preserving the data privacy of individual patients. By using the federated learning algorithm, the cloud server can effectively combine the predictions made by each edge device without directly accessing their raw data. Instead, only model updates are shared among devices during the training process, keeping sensitive patient information decentralized and secure. This distributed learning mechanism ensures that no single entity possesses complete patient data, mitigating the risk of data breaches and unauthorized access.

Federated Learning Coordinator. The Federated Learning Coordinator is responsible for coordinating the learning process between the edge devices and the cloud server. It ensures that the machine learning models on each edge device are updated regularly with the latest risk prediction algorithm. The coordinator also ensures that the predictions made by each edge device are combined in a secure and private manner using the blockchain framework. The federated learning coordinator also manages the blockchain-based smart contract that governs the interactions between the various components of the FECHD-RP framework.

Blockchain Integration. The blockchain plays a crucial role in the FECHD-RP by ensuring the security and privacy of patient data. In the FECHD-RP framework, the blockchain is used to create a decentralized system where patient data is encrypted and stored securely on the blockchain. This ensures that only authorized individuals can access the data and that patient privacy is maintained at all times. Moreover, the blockchain is also used to create a smart contract that governs the interactions between the different components of the framework, such as edge devices, cloud servers, and federated learning coordinators. The smart contract enforces the rules of the system and ensures that the data is shared in a secure and transparent manner. The blockchain also facilitates the verification and auditing of the data by providing a tamper-proof and immutable record of all transactions. This makes it possible to verify the authenticity and accuracy of the data and ensure that it has not been tampered with in any way.

4.1 Analysis of the Proposed Framework

The federated learning process involves multiple rounds of model training and aggregation. In each round, the edge devices train their local models using their local data and share only the model updates with the federated learning coordinator. The coordinator aggregates the model updates from all the edge devices and updates the global model. The updated global model is then distributed back to the edge devices for further training, and the process is repeated until convergence is achieved.

Privacy and security are critical considerations in the FECHD-RP framework. The federated learning process ensures that the local data never leaves the edge devices, and only model updates are shared with the coordinator. This framework employs various techniques, such as encryption and differential privacy, to further protect the privacy and security of the data.

The FECHD-RP utilizes both edge and cloud computing to predict the risk of heart disease in patients. The system uses blockchain technology to ensure the privacy and security of patient data. In a federated edge-cloud framework, data is processed locally on edge devices, such as wearable devices, smartphones, and medical devices, before being transmitted to a cloud server for further processing.

The use of edge devices in this system allows for real-time monitoring of patient data, which can be crucial in detecting and preventing heart disease. By processing data locally on edge devices, the system reduces the amount of data that needs to be transmitted to the cloud, reducing network traffic and improving system performance. Additionally, edge devices are often more readily available to patients than cloud servers, making them a convenient option for data collection.

The cloud server's ability to handle large-scale data processing and computational tasks is instrumental in generating a more accurate and robust risk prediction model. The vast amount of data collected from diverse edge devices enhances the overall predictive power and generalization capabilities of the model. Consequently, healthcare professionals can make better-informed decisions for individual patients and formulate more effective prevention and treatment strategies. In addition to model aggregation and training, the cloud server takes the responsibility of securely storing patient data seriously. Patient privacy is of utmost importance in healthcare, and the server employs advanced encryption techniques to safeguard sensitive information. By storing the data in an encrypted format, unauthorized parties are prevented from accessing and understanding the content to reduce the risk of data exposure or leakage.

To ensure data security and integrity, the proposed framework utilizes blockchain technology. The cloud server participates in the blockchain network, providing a transparent and tamper-resistant ledger for data transactions and model updates. This decentralized and immutable nature of the blockchain adds an extra layer of trust and accountability to the system. It assures patients and healthcare stakeholders that data is handled ethically and responsibly.

The use of blockchain technology in this system ensures the privacy and security of patient data. Blockchain technology creates a decentralized system where data is stored on multiple nodes, making it difficult for hackers to access or alter data. Each block in the blockchain contains a cryptographic hash of the previous block, ensuring the integrity of the data. In this system, patient data is

Table 2. Heart disease risk prediction methods comparison with others existing methods

Ref.	Method	Technology Used	Pros	Cons
[17]	Framingham Risk Score	Statistical Analysis	Widely used, well-validated	Requires many inputs, may not be accurate for certain populations
[20]	QRISK3	Machine Learning	Personalized risk assessment, includes socio-demographic factors	Requires many inputs, not validated in all populations
[3]	ASCVD Risk Estimator	Statistical Analysis	Widely used, includes race/ethnicity	May overestimate risk for certain populations
[4]	DeepHeart	Deep Learning	Uses ECG data for risk assessment	Requires ECG data, not widely validated
[38]	EHR-based models	Machine Learning	Uses electronic health records for risk assessment	May be limited by incomplete or inaccurate data
[18]	Wearable devices	IoT	Continuous monitoring of heart rate and other metrics	May not be accurate or reliable for all individuals
[34]	Genetic risk scores	Genetic Analysis	Personalized risk assessment based on genetic factors	May not be accurate or reliable for all individuals, limited by available genetic data
[21]	Biomarkers	Laboratory Analysis	Measures of inflammation, cholesterol, etc.	May not be widely available or affordable
[28]	Coronary artery calcium scoring	Imaging	Measures calcification in arteries	Requires imaging equipment, may not be widely available or affordable
[15]	Machine learning models using imaging data	Machine Learning	Uses imaging data for risk assessment	May require specialized equipment or expertise
[12]	Digital phenotyping	Machine Learning	Uses smartphone data for risk assessment	May not be widely validated, may require specialized technology
[2]	Risk assessment based on lifestyle factors	Statistical Analysis	Considers factors like diet, exercise, and smoking	May be limited by self-reporting bias
Proposed	Heart disease risk prediction	Federated Edge-Cloud and Blockchain	Considers factors like food calories consumed and BP level	—

encrypted and stored on the blockchain, making it accessible only to authorized parties. By using a blockchain, patients can have greater control over their own health data, which can be particularly important in the context of heart disease, which can be impacted by factors such as lifestyle and genetics.

5 Future Directions

The federated edge-cloud framework for heart disease risk prediction using blockchain is an innovative approach that utilizes the power of edge computing, cloud computing, and blockchain technology to enhance the accuracy and security of heart disease risk prediction models.

One possible future direction for this framework could be the integration of artificial intelligence (AI) and ML techniques [13]. AI and ML can be used to analyze and learn from the vast amount of data collected by the framework and to continuously improve the accuracy of heart disease risk prediction models.

Another potential direction could be the expansion of the framework to include additional health parameters and data sources, such as wearable devices, electronic health records, and medical imaging. This would allow for a more comprehensive and personalized approach to heart disease risk prediction, tailored to the unique characteristics of each individual patient.

In addition, the framework could be extended to other healthcare domains beyond heart disease, such as cancer, diabetes, and mental health. This would require adapting the framework to the specific needs and data requirements of each domain, but could ultimately lead to significant improvements in patient outcomes and population health. There is an opportunity to explore the potential of decentralized autonomous organizations (DAOs) in the context of the federated edge-cloud framework for heart disease risk prediction. DAOs could be used to govern the operation and maintenance of the framework, allowing for a more democratic and decentralized decision-making process that aligns with the values of blockchain technology. Here are the future directions for the federated edge-cloud framework for heart disease risk prediction using Blockchain:

Integration of Additional Data Sources. The framework could be expanded to include data from sources such as social media, genomics, and environmental factors. This would enable more comprehensive heart disease risk prediction models.

Personalized Medicine. The proposed framework has the potential to the personalized medicine plans for patients and enhance their individual heart disease risk factors and other health metrics. By harnessing the power of data analytics, machine learning, and real-time monitoring, the framework can offer tailored treatment strategies, ultimately improving patient outcomes and optimizing healthcare delivery.

Real-time Heart Monitoring. The proposed framework enables real-time monitoring of patients' hearts, leading to early detection and intervention for heart disease. This capability can significantly improve patient outcomes and reduce the burden of heart-related complications

Improved Collaboration Between Healthcare Providers. The federated edge-cloud framework could facilitate collaboration between healthcare providers, allowing for more accurate and comprehensive heart disease risk assessments.

Development of Patient-Facing Applications. Patient-facing applications developed within the federated edge-cloud framework have the potential to extend how patients monitor their heart health and receive personalized lifestyle recommendations. These applications can empower individuals to take a proactive role in managing their cardiovascular well-being

Integration of Blockchain-Based Consent Management. Incorporating blockchain-based consent management into the proposed federated edge-cloud framework can empower patients with greater control over their health data and enhance privacy protection. Blockchain technology offers unique features that can revolutionize consent management and data sharing in the healthcare domain

Development of New Heart Disease Risk Factors. The proposed framework has the potential to revolutionize heart disease risk prediction and prevention by identifying new and previously unknown risk factors. This capability can significantly enhance the accuracy and effectiveness of heart disease risk assessments, leading to more targeted preventive strategies and improved patient outcomes.

Real-Time Heart Disease Risk Assessment. The federated edge-cloud framework to develop real-time heart disease risk assessment tools holds immense potential in transforming how healthcare providers evaluate and manage their patients' heart health. The combination of federated learning, edge computing, and cloud resources enables the development of highly efficient and accurate risk assessment tools, providing valuable insights to healthcare professionals for timely and personalized interventions.

Integration of Telemedicine. Integrating telemedicine into the proposed blockchain-enabled federated edge-cloud framework can bring significant advantages, especially in enabling remote heart disease risk assessments and monitoring. Telemedicine, which involves using telecommunications technology to provide healthcare services remotely, offers numerous benefits for both patients and healthcare providers.

Development of New Heart Disease Prevention Strategies. The federated edge-cloud framework could be used to develop and test new heart disease prevention strategies, such as personalized nutrition plans and exercise recommendations.

6 Conclusion

Heart disease is a serious and prevalent health condition that can be managed and prevented through lifestyle changes and medical treatments. Federated learning and edge computing have shown great potential in the healthcare domain, but concerns around privacy and security remain. The proposed federated edge-cloud framework for heart disease risk prediction using blockchain technology addresses these concerns by utilizing blockchain to secure the data sharing and model aggregation process, while also providing transparency and accountability. The framework's use of edge devices and cloud servers allows for efficient data preprocessing, feature extraction, model training, and validation, while the federated learning approach ensures data privacy. However, this framework presents a promising solution for healthcare organizations and researchers who need to collaborate on machine-learning tasks while ensuring the privacy and security of sensitive medical data.

Acknowledgement. This work was supported by a 2023-2024 Faculty Research Initiative grant from the Thurgood Marshall College Fund and the Novartis US Foundation.

References

1. Abbas, S., et al.: Fused weighted federated deep extreme machine learning based on intelligent lung cancer disease prediction model for healthcare 5.0. Int. J. Intell. Syst. **2023**, Article ID 2599161, 14 (2023). https://doi.org/10.1155/2023/2599161
2. Appiah, D., Capistrant, B.D.: Cardiovascular disease risk assessment in the united states and low-and middle-income countries using predicted heart/vascular age. Sci. Reports **7**(1), 16673 (2017)
3. Azevedo, T.d.A., Moreira, M.L.V., Nucera, A.P.C.d.S.: Cardiovascular risk estimation by the ASCVD risk estimator application in a university hospital. Int. J. Cardiovasc. Sci. **31**, 492–498 (2018)
4. Ballinger, B., et al.: Deepheart: semi-supervised sequence learning for cardiovascular risk prediction. In: Proceedings of the AAAI conference on artificial intelligenc, vol. 32 (2018)
5. Cascino, T.M., et al.: Racial inequities in access to ventricular assist device and transplant persist after consideration for preferences for care: A report from the revival study. Circ.: Heart Failure **16**(1), e009745 (2023)
6. Çaydaş, U., Hasçalık, A., Ekici, S.: An adaptive neuro-fuzzy inference system (ANFIS) model for wire-EDM. Expert Syst. Appl. **36**(3), 6135–6139 (2009)
7. Chatterjee, P., Das, D., Rawat, D.B.: Use of federated learning and blockchain towards securing financial services. arXiv preprint arXiv:2303.12944 (2023)

8. Chenthara, S., Ahmed, K., Wang, H., Whittaker, F.: Security and privacy-preserving challenges of e-health solutions in cloud computing. IEEE Access **7**, 74361–74382 (2019). https://doi.org/10.1109/ACCESS.2019.2919982
9. Das, D., Banerjee, S., Dasgupta, K., Chatterjee, P., Ghosh, U., Biswas, U.: Blockchain enabled SDN framework for security management in 5g applications. In: 24th International Conference on Distributed Computing and Networking, pp. 414–419 (2023)
10. Das, D., Banerjee, S., Mansoor, W., Biswas, U., Chatterjee, P., Ghosh, U.: Design of a secure blockchain-based smart iov architecture. In: 2020 3rd International Conference on Signal Processing and Information Security (ICSPIS), pp. 1–4. IEEE (2020)
11. Dash, S., Tripathy, R.K., Dash, D.K., Panda, G., Pachori, R.B.: Multiscale domain gradient boosting models for the automated recognition of imagined vowels using multichannel eeg signals. IEEE Sensors Lett. **6**(11), 1–4 (2022)
12. DeBoever, C., Tanigawa, Y., Aguirre, M., McInnes, G., Lavertu, A., Rivas, M.A.: Assessing digital phenotyping to enhance genetic studies of human diseases. Am. J. Human Genetics **106**(5), 611–622 (2020)
13. Djenouri, Y., Belhadi, A., Srivastava, G., Ghosh, U., Chatterjee, P., Lin, J.C.W.: Fast and accurate deep learning framework for secure fault diagnosis in the industrial internet of things. IEEE Internet of Things J. (2021)
14. Franco, R.Z., Fallaize, R., Lovegrove, J.A., Hwang, F.: Popular nutrition-related mobile apps: a feature assessment. JMIR mHealth and uHealth **4**(3), e5846 (2016)
15. Guo, A., Pasque, M., Loh, F., Mann, D.L., Payne, P.R.: Heart failure diagnosis, readmission, and mortality prediction using machine learning and artificial intelligence models. Curr. Epidemiol. Reports **7**, 212–219 (2020)
16. Hasanova, H., Tufail, M., Baek, U.J., Park, J.T., Kim, M.S.: A novel blockchain-enabled heart disease prediction mechanism using machine learning. Comput. Electr. Eng. **101**, 108086 (2022). https://doi.org/10.1016/j.compeleceng.2022.108086, https://www.sciencedirect.com/science/article/pii/S004579062200341X
17. Hemann, B.A., Bimson, W.F., Taylor, A.J.: The framingham risk score: an appraisal of its benefits and limitations. Am. Heart Hospital J. **5**(2), 91–96 (2007)
18. Iqbal, S.M., Mahgoub, I., Du, E., Leavitt, M.A., Asghar, W.: Advances in healthcare wearable devices. NPJ Flexible Electron. **5**(1), 9 (2021)
19. Khan, M.A., Algarni, F.: A healthcare monitoring system for the diagnosis of heart disease in the IoMT cloud environment using MSSO-ANFIS. IEEE Access **8**, 122259–122269 (2020). https://doi.org/10.1109/ACCESS.2020.3006424
20. Livingstone, S., et al.: Effect of competing mortality risks on predictive performance of the qrisk3 cardiovascular risk prediction tool in older people and those with comorbidity: external validation population cohort study. Lancet Healthy Longevity **2**(6), e352–e361 (2021)
21. Mayeux, R.: Biomarkers: potential uses and limitations. NeuroRx **1**, 182–188 (2004)
22. Mohan, S., Thirumalai, C., Srivastava, G.: Effective heart disease prediction using hybrid machine learning techniques. IEEE Access **7**, 81542–81554 (2019). https://doi.org/10.1109/ACCESS.2019.2923707
23. Mortazavi, B.J., et al.: Analysis of machine learning techniques for heart failure readmissions. Circ.: Cardiovasc. Qual. Outcomes **9**(6), 629–640 (2016)
24. Muthu, B., et al.: A framework for extractive text summarization based on deep learning modified neural network classifier. Trans. Asian Low-Resource Lang. Inform. Process. **20**(3), 1–20 (2021)

25. Nagesh, S.H., Kumar, K.R.A., Rajgopal, K.T.: Cloud architectures encountering data security and privacy concerns - a review. In: 2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS), pp. 1729–1735 (2017). https://doi.org/10.1109/ICECDS.2017.8389745
26. Nashif, S., Raihan, M.R., Islam, M.R., Imam, M.H.: Heart disease detection by using machine learning algorithms and a real-time cardiovascular health monitoring system. World J. Eng. Technol. **6**(4), 854–873 (2018)
27. Nowbar, A.N., Gitto, M., Howard, J.P., Francis, D.P., Al-Lamee, R.: Mortality from ischemic heart disease: Analysis of data from the world health organization and coronary artery disease risk factors from NCD risk factor collaboration. Circul.: Cardiovasc. Qual. Outcomes **12**(6), e005375 (2019)
28. Pletcher, M.J., Tice, J.A., Pignone, M., Browner, W.S.: Using the coronary artery calcium score to predict coronary heart disease events: a systematic review and meta-analysis. Arch. Internal Med. **164**(12), 1285–1292 (2004)
29. Reddy, D.K.K., Nayak, J., Naik, B., Ghosh, U., Sharma, P.K.: Exact greedy algorithm based split finding approach for intrusion detection in fog-enabled IoT environment. J. Inform. Secur. Appl. **60**, 102866 (2021)
30. Sarmah, S.S.: An efficient IoT-based patient monitoring and heart disease prediction system using deep learning modified neural network. IEEE Access **8**, 135784–135797 (2020). https://doi.org/10.1109/ACCESS.2020.3007561
31. Saw, M., Saxena, T., Kaithwas, S., Yadav, R., Lal, N.: Estimation of prediction for getting heart disease using logistic regression model of machine learning. In: 2020 International Conference on Computer Communication and Informatics (ICCCI), pp. 1–6 (2020). https://doi.org/10.1109/ICCCI48352.2020.9104210
32. Simpson, C.C., Mazzeo, S.E.: Calorie counting and fitness tracking technology: Associations with eating disorder symptomatology. Eating Behav. **26**, 89–92 (2017)
33. Siva Shankar, G., Ashokkumar, P., Vinayakumar, R., Ghosh, U., Mansoor, W., Alnumay, W.S.: An embedded-based weighted feature selection algorithm for classifying web document. Wirel. Commun. Mobile Comput. **2020**, 1–10 (2020)
34. Udler, M.S., McCarthy, M.I., Florez, J.C., Mahajan, A.: Genetic risk scores for diabetes diagnosis and precision medicine. Endocrine Rev. **40**(6), 1500–1520 (2019)
35. Virani, S.S., et al.: Heart disease and stroke statistics-2020 update: a report from the American heart association. Circ.: Heart Failure 141(9), e139–e596 (2020)
36. Yaqoob, M.M., Nazir, M., Khan, M.A., Qureshi, S., Al-Rasheed, A.: Hybrid classifier-based federated learning in health service providers for cardiovascular disease prediction. Appl. Sci. **13**(3) (2023). https://doi.org/10.3390/app13031911, https://www.mdpi.com/2076-3417/13/3/1911
37. Yuan, X., Chen, J., Zhang, K., Wu, Y., Yang, T.: A stable AI-based binary and multiple class heart disease prediction model for IoMT. IEEE Trans. Indust. Inform. **18**(3), 2032–2040 (2022). https://doi.org/10.1109/TII.2021.3098306
38. Zeng, Z., Deng, Y., Li, X., Naumann, T., Luo, Y.: Natural language processing for EHR-based computational phenotyping. IEEE/ACM Trans. Comput. Biol. Bioinform. **16**(1), 139–153 (2018)

Cyber Security/Privacy/Trust for IoT and CPS (SPT)

Understanding Cybersecurity Challenges and Detection Algorithms for False Data Injection Attacks in Smart Grids

Pallavi Zambare(✉) and Ying Liu(✉)

Texas Tech University, Lubbock, USA
{pzambare,Y.Liu}@ttu.edu

Abstract. In Smart grid (SG), cyber-physical attacks (CPA) are the most critical hurdles to the use and development. False data injection attack (FDIA) is a main group among these threats, with a broad range of methods and consequences that have been widely documented in recent years. To overcome this challenge, several recognition processes have been developed in current years. These algorithms are mainly classified into model-based algorithms or data-driven algorithms. By categorizing these algorithms and discussing the advantages and disadvantages of each group, this analysis provides an intensive overview of them. The Chapter begins by introducing different types of CPA as well as the major stated incidents history. In addition, the chapter describes the use of Machine Learning (ML) techniques to distinguish false injection attacks in Smart Grids. A few remarks are made in the conclusion as to what should be considered when developing forthcoming recognition algorithms for fake data injection attacks.

Keywords: Smart grid · False data injection attacks · Machine learning Models · Data-driven detection algorithms · CPA · Model-based detection algorithms

1 Introduction

Intelligent systems that integrate designed that incorporate networks of physical and computational mechanisms are known as cyber-physical systems (CPS) [1,7] in vital infrastructures like electric power systems, water systems, health care, home automation, and transportation, in addition to completely networked and integrated systems. A CPS is a collection of complicated control, computing, awareness, and communication systems. The complexity and variety of CPSs have revealed potential threats to their security and resilience. The interconnectivity of bulk physical layer components makes it more difficult to guard against physical vulnerabilities. Because cyber incorporation trusts on network connections and Internet of Things (IoT)-based machines, significant insurances in security designs and improvements are required to defend against unanticipated cyber-attacks [2]. A CP assault is a cyber-security violation that has a

Published by Springer Nature Switzerland AG 2024
D. Puthal et al. (Eds.): IFIPIoT 2023, IFIP AICT 684, pp. 333–346, 2024.
https://doi.org/10.1007/978-3-031-45882-8_22

negative impact on a CPS's physical environment [3]. By combining cyber and physical environments in a CPS, CPA risks information confidentiality, integrity, and availability. Several notable CPA have been documented in the sector in recent decades, facilitating synergistic efforts by industry practitioners and academic groups to usher in a new age of CPS security.

1.1 History of Cyber-Physical Attacks in Energy Sector

Over the last few decades, CPA has been recorded in the energy sector. It began in 1982, with the declaration of the first major attack. These attacks have a wide variety of consequences. Some remained undiscovered, while others resulted in explosions, millions of dollars in damages, and even lives. The true danger is the rise in the number of such instances. Between 2011 and 2014, the US Energy Department received 362 complaints of power outages caused by CPA; 161 occurrences were recorded in 2013, associated with 31 cases in 2011 [20]. Comparable to the 2017 level of industrial cybersecurity study, 54% of analyzed companies (359 in 21 countries) experienced a cyber-physical security concern last year, and 21% had two [4].

A major pipeline explosion happened in the Siberian tundra in 1982. Details of the explosion were gleaned from the recollections of US officials during the Cold War. The CIA seems to have purposefully tampered with the gas pipeline control software, causing valves to malfunction, subsequent in extreme pressure crossings and large explosion [1].

In 2003, a Slammer worm got into the computer network of the David-Besse nuclear power station in Ohio, USA, via the contractor's network. For five hours, security parameters and indicators were disabled due to this penetration. Thus, the engineers in the control room couldn't monitor crucial parameters, such as the core temperature of the reactor [7].

The US Department of Homeland Security initiated the Aurora cyberattack in 2007. As a result of the attack, a hacker gained access to a test generator's control system, compelling it to quickly toggle between on and off its electrical circuit breakers. There was a significant synchronization problem between the mechanical and electrical system of the generators, which resulted in the explosion of a $1 million generator used across the United States [19]

For several hours on December 23, 2015, Kiev, Ukraine experienced a major blackout. Over 225,000 people were affected by the blackout [32]. A six-month investigation into the mysterious black-out led to the conclusion that foreign cyber-attacks were involved. The attack impacted seven 110 kV and 23 kV substations. As a result of compromising the Administrative Control and Data Acquisition system, hackers were able to open many circuit breakers in the distribution system. Consequently, the machinists were unable to contact the SCADA system and were forced to manually repair the circuit sides [20]

In 2014, the "National Institute of Standards and Technology (NIST) released a three-volume paper laying out fundamentals of smart grid cyber security" [31].

1.2 Cyber-Physical Systems of Smart Grid Architecture

The existing smart grid (SG) is constructed on the interdependence of cyber-physical (CP) networks. Figure 1 depicts SG's typical multi-layer architecture, which comprises physical, data collecting, communication, and application levels. Generating, transmission, and distribution networks make up the physical layer [7] Distributed energy resources (DERs) include solar, wind, and hydroelectric energy, which are linked to grid through converters to achieve maximum power output [2]. Smart sensors and measuring equipment make up the data acquisition layer, which collects data and sends it to the communication layer. The energy management system (EMS), which optimizes, monitors, and regulates the actuators, receives data from these devices.

While cyber layers increase SG's efficiency, they also increase its vulnerability by widening the attack surface. Attackers may get access to vulnerable areas, causing monitoring and control of physical equipment to be disrupted. The SG network contains a number of significant characteristics, including necessary reaction, energy efficiency, a dynamic power marketplace, and distributed computerization [8]. SG is a complicated network because of these distinguishing characteristics.

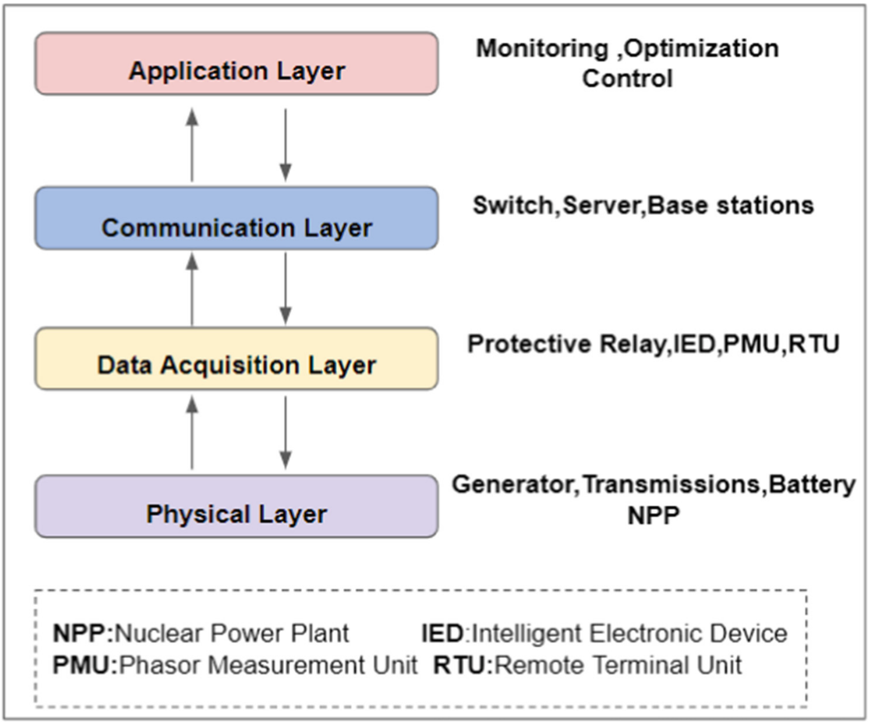


Fig. 1. Architecture of the cyber-physical systems of smart grid [28].

1.3 Smart Grid Vulnerabilities

A smart grid network's vulnerability is pointed at an attacker who might gain access to the system and launch an attack. Smart grid is vulnerable to many cyberattacks [30] since it links to multiple domains via different protocols.

Conditions that might render the grid more susceptible to cyber-attacks. Attacks may be categorized into 2 classes: passive and aggressive. Active attacks are more harmful because the attacker affects data or stops the recipient from getting it [10], while passive attacks do not destroy the data but the attacker watches it.

Eavesdropping and traffic analysis assaults are the two types of passive attacks. Masquerade, fake data injection, replay, and DOS attacks are examples of active attacks. An eavesdropping attack allows the attacker to monitor data packets exchanged among the source and beneficiary. The attacker, on the other hand, It doesn't alter the data. A traffic analysis attack, for example, is one that monitors and analyzes traffic between a sender and a recipient. Active attacks are more damaging than passive attacks since the attacker have complete control over the data. [29].

When the attacker and the sender both transmit data to the receiver, the recipient becomes confused about the difference between actual data sent by the sender and data routed via the attacker. A receiver receives data from the sender while the sender is inactive in a masquerade attack [17].

False data injection happens when data is sent from sender to receiver, but the recipient gets changed data directly from the attacker. The sender and recipient, on the other hand, are completely oblivious to the attacker's alteration. The attacker does not target the transmitter or recipient, but rather the data server in a denial-of-service assault. The attacker sends the server a large number of unrelated requests, which the server then serves until it runs out of resources [20].

The following are the primary factors that make smart grid susceptible to cyber-attacks [30]:

1. More intelligent electronic devices (IEDs) are being installed: The larger number of devices in the network, beyond the number of attack spots accessible to attackers. Even if just one point is hacked, the whole network system is affected.
2. Installing third-party components without consulting experts increases the vulnerability of the network to cyberattacks. Trojans might infect the devices, which would then propagate to other devices on the network.
3. Inadequate employee training: To operate any technology, proper training is required. Employees who have not received enough training are in danger of falling victim to phishing assaults.
4. Using Internet protocols: When it comes to data transfer, not all methods are secure. Unencrypted data transmission is used by several protocols. Man-in-the-middle attacks may be used to extract data due to this.
5. Maintenance: Although the primary objective of maintenance is to keep on running things smoothly, it may sometimes be used as a vector for cyberattacks. Operators test the security system by disabling it during maintenance.

Electric power providers in Eastern Europe reported a similar incident in 2015.

1.4 Smart Grid Security Challenges

In a smart grid, cybersecurity and complexity pose the two most significant challenges. When smart grid data is presented on the cloud, these issues become more challenging [2]. Cybersecurity Is becoming a key factor of smart grid security to make certain it is always stable and assured. Cybersecurity is not only essential for smart grids but demonstrates still conventional and non-smart grids are susceptible to cyberattacks. Figure 2 classifies the Security Challenges in Smart Grid. Smart grid cybersecurity challenges are divided into five main categories below

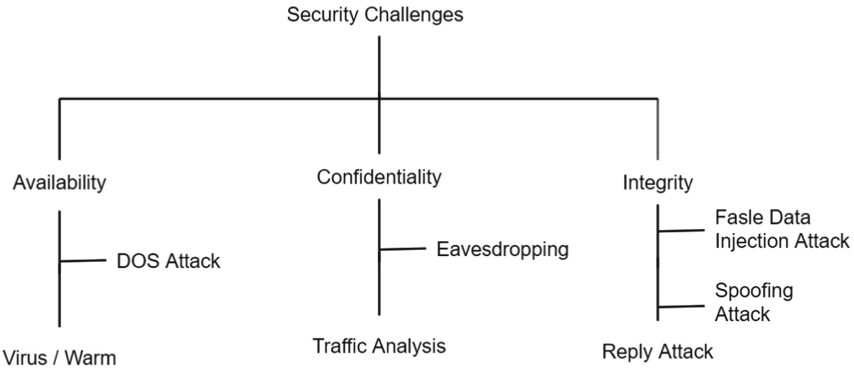


Fig. 2. Security Challenges in Smart Grid

Authentication: The user's identification. It checks if the user's credentials are valid and whether the information given by the user is correct. The [30] presents several authentication strategies in the smart grid network.

Authorization: After providing the correct credentials, the user will be authenticated. Credentials entered by the users during an unencrypted authentication process are exposed to the attacker, who then utilizes the credentials to impersonate to be a legitimate user.

Confidentiality: Authorized users have access to data. The smart grid network transmits a large amount of sensitive data. This data includes consumer energy usage measurements, consumer identification information, and a list of appliances in process. An attacker might utilize these facts to figure out the energy consumption patterns of customers. Furthermore, If unauthorized individuals gain entry to the data, an Internet Control Message Protocol (ICMP) flood assault may be released, altering or changing the reading [19]. As a result, users may possibly face major financial difficulties, and consumers might be forced to pay outrageous prices.

Integrity: Data is neither modified nor corrupted while being transferred, protecting the receiver from meddling. Checksum error, Parity check, k and other similar methods are employed to ensure data integrity at the receiving end. One of the most popular types of attack is the fake data injection attack (FDIA) [13]. Genuine data is modified and replaced with false data in an injection attack.

Availability: Availability assurances that sources or information are always accessible when a user demands them. There are a variety of issues that might influence availability, including data center failures. However, attacks like denial of service (DoS) attacks also affect cybersecurity. In DoS attacks, attackers hijack resources and deny user requests due to limited resources.

ML is a ubiquitous prominent tool that can extract patterns from any complex network data without explicit programming. Researchers are currently utilizing ML to analyze the cybersecurity of SG [10].

The evaluation was focused on a particular assault, although it did include research on the usage of ML in the electrical power system. This survey Chapter gives a general idea of current state-of-the-art ML detection techniques in the SG. ML-based security risks are examined in this chapter, and security solutions are offered to make the SG more resilient to these threats.

The rest of this chapter is arranged as mentioned below. Cyber-physical security is surveyed in Sect. 1 of the chapter. False data injection detection algorithms for the smart grid, as well as ML-based FDIA detection mechanisms, are described in Sect. 2. As a result, Sect 3 discusses the problems and opportunities of cyber-physical security in the context of the smart grid. Section 4 provides some closing remarks.

2 Research Overview

Several studies, notably FDIA in smart grids, have attempted to better comprehend and combine the different CPA. Providing a high-level overview of the most pressing cybersecurity concerns in smart grids. Figure 3 shows the classification of detection algorithm for FDIA.

2.1 FDIA Detection Algorithms in Smart Grid

In order to identify FDIA in smart grids, many approaches have been attempted. There are two fundamental motifs that emerge from these very different orientations. Model-based FDIA detection algorithms and data-driven FDIA detection algorithms are the two types.

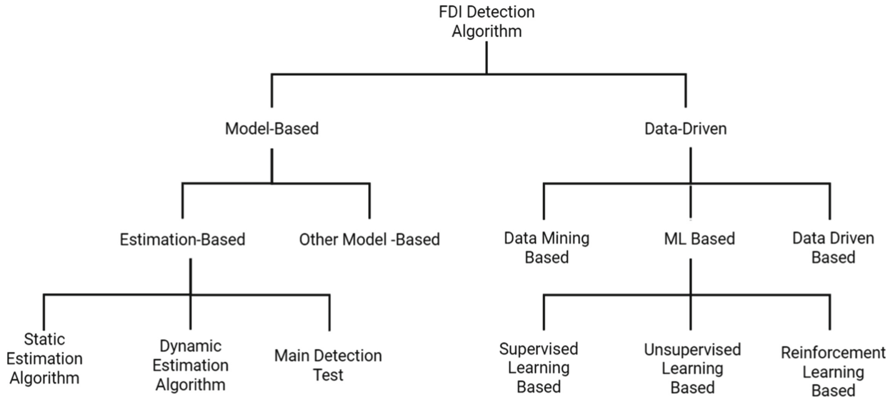


Fig. 3. Classification of Detection Algorithm for False Data Injection Attack

Model-Based Detection Algorithms: Smart grids are designed by combining real-time measurements with constant data, including system parameters and substation configurations. FDIA is the interruption of measurements or data with the intent of misrepresenting. The smart grid's model might be quasi-static or dynamic in nature, depending on the operating conditions [21].

1. The quasi-static model demonstrates a condition in which the managing points of the system modify in a smooth and constant way, with the system's controllers reacting promptly.
2. A dynamic model is used to account for dynamical changes in the scheme. The conditions of the system are based not only on present dimensions and data but also on previous states of a system in this modeling technique.

Model-Based FDIA Detection Algorithms are further classified into two groups Estimation-based detection algorithms and other model-based algorithms.

1. Estimation-based Detection Algorithm
   Estimation-based FDIA identification methods depend upon two phases:
   1) calculating state projections or estimates,
   2) evaluating findings to these states' metrics.

   However, direct calculation methods differ on dimensions and system parameters to precisely detect FDI attacks, so no estimates are needed. Several sets of dimensions across the whole power grid, as well as the system model and parameters, are used to estimate the grid's condition [14]. Traditional approaches to estimating the states of power systems utilized the Weighted Least Squares estimator. This is based on the premise that the power system will be stable and redundant enough. Real-world power systems, on the other hand, are not in a steady state due to stochastic fluctuations in demand and generation [13].

   (a) Static Estimation Methods
   Every step of the estimation process is handled independently of the previous step. This prevents the information from being passed on to the

next step. In most cases, static state estimation is used to detect FDIAs. Weighted Least Squares estimator estimation is an important component of this approach. A Weighted Least Squares estimator was used to detect FDIA in [2,10], which would misrepresent the operator into measuring the incorrect voltage and misconstruing topology changes [23].

(b) Dynamic Estimation Methods
Kalman filter (KF) has become the preferred technique in this area for updating the estimate of the state dynamically. Every estimating phase in KF involves two stages. Initially, a state prediction is made based on the state of the preceding step. The state's forecast is then corrected using the measurements that were acquired in the following stage. This method also uses previous data, but it does so using data from the current period also [24].

(c) Main Detection test
The detection test method is used as a means of detecting the FDIA after an estimation process has been conducted. Essentially, comparing anticipated states to actual grid measurements. Based on comparing the distance between the residual and Euclidean distance, some research utilizes straight-forward residual [15].

2. Other Model-Based Algorithms
In addition to model-based methods, there are other estimation-free strategies accessible in this sector. The algorithm is based on the system's model or parameters. [22] It was difficult to detect FDIA in microgrid control systems. Proposed using cooperative vulnerability factor (CVF) in [16]. When the system is free of FDIA, the resulting output of voltage controllers, is called CVF. According to [16], matrix separation (MS) was developed to identify FDIA by separating the nominal grid state and the anomalies matrix (Table 1).

Table 1. Benefits and drawbacks of False data Injection attack detection algorithms

Algorithm	Advantages	Disadvantages
Model-based Detection Algorithms	– Training is not required – Previous data is not required – Reduced memory consumption	– Threshold determination – An unexpectedly long detection delay – Potential divergences – System modeling is needed – System parameters are required
Data-driven Detection Algorithms	– Fast process of detection – Compatibility with real-time – Easily Scalable – Unaffected by system and parameter	– Training is essential – Preparation of training data (labeled and unlabeled) – Memory space needs to be increased. – Overfitting the training data

Data Driven Detection Algorithms: Data-driven detection algorithms, distinct from model-based detection algorithms, do not use system parameters or models. These algorithms may be classified into three primary types based on how they use data to identify FDIA in smart grids:

1. Machine learning algorithms
2. Data mining algorithms
3. Other algorithms that do not involve learning or mining in them.

1. Machine learning-based Algorithms
   In the field of artificial intelligence, ML is a broad term. With ML, we can use taught computers to do complex tasks like detecting FDI attacks in smart grids. ML-based algorithms, and different model-based FDI attack detection techniques, are established on data gained from the system. For the machine to learn, a data-driven strategy demands a substantial dependence on past data from the system under evaluation. Unsupervised, supervised, and reinforcement learning approaches are among ML-based detection algorithms [16].

   (a) Supervised learning
   The mapping of inputs and outputs is explored to anticipate new inputs' outcomes. It is supervised learning in which labeled data is utilized to train a computer. The algorithm's primary flaws are the kernel function and the need for a lot of CPU time throughout training [16].

   (b) Unsupervised learning
   An ML class that uses unlabeled data to capture data similarity and difference. Unsupervised learning uses unlabeled data to find unknown classification methods and patterns. Therefore, the machine's job is to analyze hidden features of data points and divide them into classes. The FDIA in smart grids can be detected by using this approach as smart grids have different classes from the normal ones. There are a number of unsupervised learning algorithms that can be used to detect FDIAs in smart grids. An algorithm for unsupervised learning KMC is a widely utilized and well-liked strategy in classification difficulties [23].
   A soft clustering is an expanded form of clustering where an experiment can be part of more than one cluster with different grades. As a result, the clusters could overlap instead of having barely defined boundaries in the clustering process. This method was utilized to detect FDIA, giving slightly better detection accuracy than the KMC method.

   (c) Reinforcement learning
   It differs from supervised and unsupervised learning since it uses intelligent agents to optimize cumulative reward. By analyzing its prior behaviors, the machine may learn the best path of action. Unlike supervised learning, where sample data is utilized to train, mistakes are noted in reinforcement learning. Thus, a series of excellent choices will be "reinforced" as it solves the issue well. This type of learning, unlike supervised and unsupervised learning, requires further investigation into FDI attack detection in smart grids. This is due to the insufficient literature mentioned in [17].

2. Data Mining-Based Algorithms
   In data mining, enormous data sets are searched for patterns. We can analyze variable measurements collected from a system using data mining techniques based on hidden patterns or qualities. The interdisciplinary nature of data mining makes it a form of statistics and ML. In fact, unsupervised ML algorithms are often regarded as part of data mining algorithms. This manuscript, however, separates these algorithms from ML since the literature segregates them from ML. Due to their few applications in this field, FDIA detection techniques based on data mining are deemed premature. A few approaches have nonetheless been tested [18].

3. Data-Driven Algorithms
   Other data-driven FDIA detection techniques aren't specifically defined as ML or data mining. In the classification phase, the algorithm categorizes data points into regular and irregular depending on the distance. These generalized examples have the benefit of using less memory since just their specifics are required to be preserved. FDIA detection employs signal temporal logic (STL), which compares DC voltages and currents to higher and lower bounds [19] used PCA.

2.2 ML-Based FDIA Detection Methods

Using ML, the majority of the research was aimed at detecting stealthy FDI attacks.Table 2. summaries An Overview of ML-Based FDI attack detection techniques in Smart Grid. Esmalifalak et al. investigated the detection of stealthy FDI threats using an SVM-based approach and statistical anomaly detection method [5]. When sufficiently large numbers of data are collected, an SVM-based model outperforms a statistical approach.

Using artificial neural networks and fine-grained data from smart meters, Vitaly et al. developed a unique application of a ML approach to analyze energy usage data to report energy fraud [6]. In contrast to similar techniques applied in the field, our approach detects more forms of fraud by identifying unauthorized energy usage. The authors introduced a detection approach based on a conditional deep belief network (CDBfN) that abstracts temporal information from dispersed sensor readings [23]. Despite attacks on measurements and noise from the environment, the proposed detection scheme remains robust. Moreover, it is more accurate than SVM and AI-based methods such as Artificial Neural Networks (ANN). Karimipour et al. presented an independent, continuous, and computationally efficient method for detecting FDI attacks [26]. This method employs a feature mining scheme and a time series splitting algorithm.

For the detection of unobservable attacks, they examined the Bayesian Dynamic Network (DBsN) concept and Boltzmann machine learning-based algorithms. Valdes et al. presented a novel intrusion detection method (IDM) for substation distribution systems using self-organizing maps (SOM) and adaptive resonance theory (ART) to distinguish between normal, fault, and attack states [11].

Table 2. An Overview of ML-Based FDI attack detection techniques in Smart Grid

Reference	ML Algorithm	ML Model	Approach	Testbed	Performance Accuracy
Esmalifalak et al. [5]	SVM	S	Stealthy False Data Injection is detected by supervised learning using labeled data and training a distributed support vector machine	IEEE 118 bus	99% accuracy
Vitaly et al. [6]	ANN	S	Fraud detection in smart grids using artificial neural networks and fine-grained energy meter data	NA	87% accuracy
Jun Yan et al. [8]	kNN	S	The detection of FDI attacks as binary classification problems and combined three algorithms: Support vector machine, extended nearest neighbor (ENN) and K-nearest neighbor (KNN)	IEEE 30 bus	100%accuracy
Alfonso et al. [9]	ART and SOM based classifier (Novel)	U	Method of detecting intrusion in substation distribution systems using ART and SOM to distinguish between common, fault, and attack states	RTDS hardware	90%accuracy
H.M. Kalid et al. [11]	CDBfN	S	An algorithm that uses a CDBfN to extract the temporal characteristics of distributed sensor measurements.	IEEE 118, 300 bus	98%accuracy
Abdelrahman et al. [20]	RNN	S	The RNN detects FDI attacks by analyzing the correlations between measurements across time and space in contrast to other methods of learning	IEEE 30 bus	99%accuracy
Hadis et al. [24]	DBsN	S	Detecting Smart Grid cyber-attacks using heuristkarimipour2019deepics and a time-series partitioning algorithm	IEEE 118, and 2848 bus	99%accuracy
Xiangyu et al. [25]	CNN and LSTM	S	An efficient method of dynamic finding of false data injection attacks in smart grids employing a CNN and a LSTM network	IEEE 39 bus	90%accuracy
Mohammad Reza et al. [26]	NARX ANN	S	In both transient and steady-state situations, NARX neural networks can accurately identify FDI attacks	DC microgrid system	95%accuracy
Chenguang et al. [27]	Autoencoder ANN	S	False data injection detection using the autoencoder approach with unbalanced training data	IEEE 118 bus	95%accuracy

S *:Supervised machine learning model,* ***U*** *: Unsupervised machine learning model*

Yan et al. examined the detection of FDI attacks as binary classification problems and combined three algorithms: K-nearest neighbor (KNN), extended nearest neighbor (ENN), and Support vector machine (SVM)[8], According to their experimental analysis, It is possible to optimize all of these algorithms to detect FDI attacks effectively. According to Ayad et al., recurrent neural networks (RNNs) can identify FDI attacks using the correlation between measurements across time and space, unlike other learning methods [20]. An artificial intelligence-based system consisting of a long short-term memory (LSTM) and a convolution neural network (CNN), the network was presented by Niu et al. to detect novel FDI attacks [25].

According to Sakhnini et al., a genetic algorithm (GA) was used to detect the best feature selection method when using three different algorithms (e.g., ANN, KNN, and SVM) with varying features. As demonstrated in [6], the proposed methods use nonlinear autoregressive exogenous (NARX) neural networks to accurately identify FDI attacks both in transient and steady-state situations. The autoencoder artificial neural networks have also been used by Wang et al. [27]to detect FDI attacks.

3 Research Problems

This assessment recognized the remaining difficulties as potential research pillars:

- The effect of uncertainties on system parameters, modeling, and measurements.
- Smart grids have a dynamic nature due to the different states and operation conditions. It is important to pay more attention to the fluctuating nature of the distribution systems, specifically with the modern trend of delivered generation and microgrids.
- Smart grids generate a huge amount of data, which increases computational complexity

Future FDIA detection methods must meet the following requirements:

- Compatibility with existing grid standards, protocols, and systems
- Ensures the least amount of damage from the FDIA with a high detection speed.
- Selectivity to detect the FDIA-affected metrics
- Analyze the scalability of smart grids so that they can cover such a vast number of nodes.

4 Conclusion

ML has been introducing several possibilities for all types of attackers and defenders in terms of scalability and accuracy because of its vast range of use cases in SG. In this way, it makes researchers aware of the importance of applying emerging machine-learning algorithms to security-related investigations. A review of the history, impact, and variety of the FDIA illustrates the need for advancements in detection algorithms. The detection of FDI attacks in smart grids has been varied. Some are model-dependent, others data-driven. There are pros and cons to each of these categories. Additionally, we provide a tabular form that summarizes the various studies in an organized manner so that future researchers may better focus on those areas that need further study. The goal should be to create an algorithm with the fewest possible drawbacks.

References

1. Reed, T.: At the Abyss: An Insider's History of the Cold War. Presidio Press, Novato (2005)
2. Hardy, T.L.: Software and System Safety: Accidents, Incidents, and Lessons Learned. AuthorHouse, Bloomington (2012)
3. Swearingen, M., Brunasso, S., Weiss, J., Huber, D.: What You Need to Know (and Don't) About the AURORA Vulnerability. PowerMag (2013)
4. Manandhar, K., Cao, X., Hu, F., Liu, Y.: Detection of faults and attacks including false data injection attack in smart grid using Kalman filter. IEEE Trans. Control Netw. Syst. **1**(4), 370–379 (2014)
5. Esmalifalak, M., Han, Z.: Detecting stealthy false data injection using machine learning in smart grid. IEEE Syst. J. **11**(3), 1644–1652 (2014)
6. Ford, V., Siraj, A., Eberle, W.: Smart grid energy fraud detection using artificial neural networks. In: IEEE Symposium on Computational Intelligence Applications in Smart Grid (CIASG), pp. 1–6. IEEE (2014)
7. Toppa, S.: The National Power Grid Is Under Almost Continuous Attack, Report Says, Time.com (2015). https://bit.ly/1FH246I
8. Yan, J., Tang, B., He, H.: Detection of false data attacks in smart grid with supervised learning. In: International Joint Conference on Neural Networks (IJCNN), pp. 1395–1402. IEEE (2016)
9. Valdes, A., Macwan, R., Backes, M.: Anomaly detection in electrical substation circuits via unsupervised machine learning. In: IEEE 17th International Conference on Information Reuse and Integration (IRI), pp. 500–505. IEEE (2016)
10. Jiang, Y., Hui, Q.: Kalman filter with diffusion strategies for detecting power grid false data injection attacks. In: IEEE International Conference on Electro Information Technology (EIT) (2017)
11. Khalid, H.M., Peng, J.C.-H.: Immunity toward data-injection attacks using multisensor track fusion-based model prediction. IEEE Trans. Smart Grid **8**(2), 697–707 (2017)
12. Jiang, Q., Chen, H., Xie, L., Wang, K.: Real-time detection of false data injection attack using residual prewhitening in smart grid network. In: IEEE International Conference on Smart Grid Communications (SmartGridComm) (2017)
13. Chung, H.-M., Li, W.-T., Yuen, C., Chung, W.-H., Wen, C.-K.: Local cyber-physical attack with leveraging detection in smart grid. In: IEEE International Conference on Smart Grid Communications (SmartGridComm) (2017)
14. Shi, W., Wang, Y., Jin, Q., Ma, J.: PDL: an efficient prediction-based false data injection attack detection and location in smart grid. In: IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC) (2018)
15. Sahoo, S., Mishra, S., Peng, J.C.-H., Dragicevic, T.: A stealth cyber attack detection strategy for DC microgrids. IEEE Trans. Power Electron. (2018, in press)
16. Kubo, R.: Detection and mitigation of false data injection attacks for secure interactive networked control systems. In: IEEE International Conference on Intelligence and Safety for Robotics (ISR) (2018)
17. Kurt, M.N., Ogundijo, O., Li, C., Wang, X.: Online cyber-attack detection in smart grid: a reinforcement learning approach. IEEE Trans. Smart Grid, 1–12 (2018, in press)
18. Adhikari, U., Morris, T.H., Pan, S.: Applying non-nested generalized exemplars classification for cyber-power event and intrusion detection. IEEE Trans. Smart Grid **9**(5), 3928–3941 (2018)

19. Beg, O.A., Nguyen, L.V., Johnson, T.T., Davoudi, A.: Signal temporal logic-based attack detection in DC microgrids. IEEE Trans. Smart Grid (2018, in press)
20. Ayad, A., Farag, H.E.Z., Youssef, A., El-Saadany, E.F.: Detection of false data injection attacks in smart grids using recurrent neural networks. In: 2018 IEEE Power and Energy Society Innovative Smart Grid Technologies Conference (ISGT), pp. 1–5. IEEE (2018)
21. Zhao, J., Gómez-Expósito, A.: Power system dynamic state estimation: motivations, definitions, methodologies, and future work. IEEE Trans. Power Syst. **34**(4), 3188–3198 (2019)
22. Kurt, M.N., Yılmaz, Y., Wang, X.: Real-time detection of hybrid and stealthy cyber-attacks in smart grid. IEEE Trans. Inf. Forensics Secur. **14**(2), 498–513 (2019)
23. Zanetti, M., Jamhour, E., Chueiri, I.: A tunable fraud detection system for advanced metering infrastructure using short-lived patterns. IEEE Trans. Smart Grid **10**(1), 830–840 (2019)
24. Karimipour, H., Choo, K.K.R., Leung, H.: A deep and scalable unsupervised machine learning system for cyber-attack detection in large-scale smart grids. IEEE Access **7**, 80778–80788 (2019)
25. Niu, X., Tomsovic, K.: Dynamic detection of false data injection attack in smart grid using deep learning. In: 2019 IEEE Power and Energy Society Innovative Smart Grid Technologies Conference (ISGT), pp. 1–6. IEEE (2019)
26. Habibi, M.R., Blaabjerg, F., et al.: Detection of false data injection cyber-attacks in DC microgrids based on recurrent neural networks. IEEE J. Emerg. Sel. Top. Power Electron. (2020)
27. Wang, C., Tindemans, S., Palensky, P.: Detection of false data injection attacks using the autoencoder approach. arXiv preprint arXiv:2003.02229 (2020)
28. Haque, N.I., Shahriar, Md.H., Dastgir, Md.G.: Machine learning in generation, detection, and mitigation of cyberattacks in smart grid: a survey. arXiv:2010.00661v1 [cs.CR] (2020)
29. Haque, N.I., et al.: Machine learning in generation, detection, and mitigation of cyberattacks in smart grid: a survey. arXiv preprint arXiv:2010.00661 (2020)
30. Tufail, S., Parvez, I., Batool, S., Sarwat, A.: Detection, and Mitigation Techniques for the Smart Grid, Energies, A Survey on Cybersecurity Challenges (2021)
31. Guidelines for Smart Grid Cybersecurity, National Institute of Standards and Technology (2014)
32. Analysis of the Cyber Attack on the Ukrainian Power Grid, Electricity Information Sharing and Analysis Center (2016)

Comprehensive Survey of Machine Learning Techniques for Detecting and Preventing Network Layer DoS Attacks

Niraj Prasad Bhatta, Ashutosh Ghimire, Al Amin Hossain,
and Fathi Amsaad(✉)

Wright State University, Dayton, OH 45435, USA
{bhatta.8,ghimire.18,hossain.116,fathi.amsaad}@wright.edu

Abstract. With the increasing reliance on computer networks in our daily lives, the threat of network layer DoS (Denial of Service) attacks has become more prevalent. Attackers use various techniques to disrupt network services and cause loss of data, revenue, and reputation. Recent development in machine learning approaches have shown promise in prevention and detection of such types of attacks by several orders of magnitude. In this paper a thorough overview of machine learning approaches for detecting and preventing network layer DoS attacks is presented. Firstly, the basics of network layer DoS attacks, their classification, and the impact of these attacks is discussed. Then, different machine learning techniques and the ways in which they can be utilized for attack detection and prevention is explored. Additionally, analysis on the strengths and limitations of each approach, and provide a comparative study of the most relevant works in this field is done. Finally, some obstacles in research and potential avenues for future exploration is presented. in the field of machine learning-based defense mechanisms against network layer DoS attacks is discussed. In this paper a detailed summary of the most up-to-date advancements or developments in machine learning-based defense mechanisms against network layer DoS attacks is shown and serve as a reference for one and all who are involved in this field.

Keywords: DOS attack · Machine Learning · Network layer · Detection

1 Introduction

At the outset of millennium, rising usage of Computer networks has brought about a significant escalation in the Volume and intricacy of network layer attacks. The primary goal of the attack is to stop a normal operation of a network by inundating it with an overwhelming volume of traffic or deluging it with resource-intensive requests. Dos attack create a severe vulnerability to

D. Puthal et al. (Eds.): IFIPIoT 2023, IFIP AICT 684, pp. 347–356, 2024.
https://doi.org/10.1007/978-3-031-45882-8_23

the reliability, accessibility, and protection of interconnected systems Which can result in adverse consequences on both enterprises and individuals [1,2]. Novel research for identifying and preventing network layer DoS attacks to manage this burgeoning issue are proposed. Specifically, Machine learning have become a viable method for Detecting and alleviating DOS attacks, owing to their capability to analyze previous network traffic patterns and identify unusual activities [3,4].

OSI represents open Systems Interconnection is a conceptual type diagram that describes how a computer or communications network communicates. There are seven levels total, and each one defines a particular set of protocols and functions [5]. A DoS attack refers to a malevolent effort to obstruct authorized users from accessing a network resource, such as a website or server, by overwhelming it with traffic or exploiting vulnerabilities in its communication protocols [6]. where multiple compromised systems are used to flood a targeted website or network with a large amount of traffic, overwhelming its capacity and causing it to become inaccessible to legitimate users [7].

Other sections are laid out as follows: Sect. 2, summarize DoS attacks targeting network layer, including their definition, types, and impact. Section 2, summarize network layer DoS attacks, including their definition, types, and impact. Section 3, we explore the machine learning approaches that are considered as alternatives for detecting DoS attacks targeting network layer. Section 4, machine learning techniques that have been proposed for preventing network layer DoS attacks IS discussed. Section 5, a comparison between various techniques based on novel concepts of ML to identify and hinder DoS attacks targeting on network layer is provided. Section 6, Identification of open research challenges and future directions for the field is provided. In conclusion, the paper ends with a discussion on Sect. 7 (Fig. 1).

2 DoS Attacks in Network Layer

Internet protocol consists of layer that pertains to the network stack provides logical addressing and routing services that enable communication between different networks. However, the network layer is susceptible to a range of DoS attacks that have the potential to cause disturbance or interruption. the availability and performance of network services. This section provides an overview of network layer DoS attacks, including their definition, types, attack methods, and impact on network security. attacks focuses on disrupting the functionality of the IP protocol stack's network layer to overwhelm infrastructure of the network with a flood of traffic, requests, or packets. The objective of these attacks is to deplete the network's resources, disrupt the network connectivity, or cause the target system to crash or freeze [8].

2.1 The Following Are Some Common Types of Network Layer DoS Attacks

IP Spoofing. In this category of attack, the attacker falsifies the original IP address of the packet to make it appear as if it is coming from a legitimate source. By doing so, the attacker can bypass the network security measures that rely on IP address filtering or authentication.

ICMP Flood. The attacker inundates the destinated system with a flood of ICMP packets, which can consume the network bandwidth and resources.

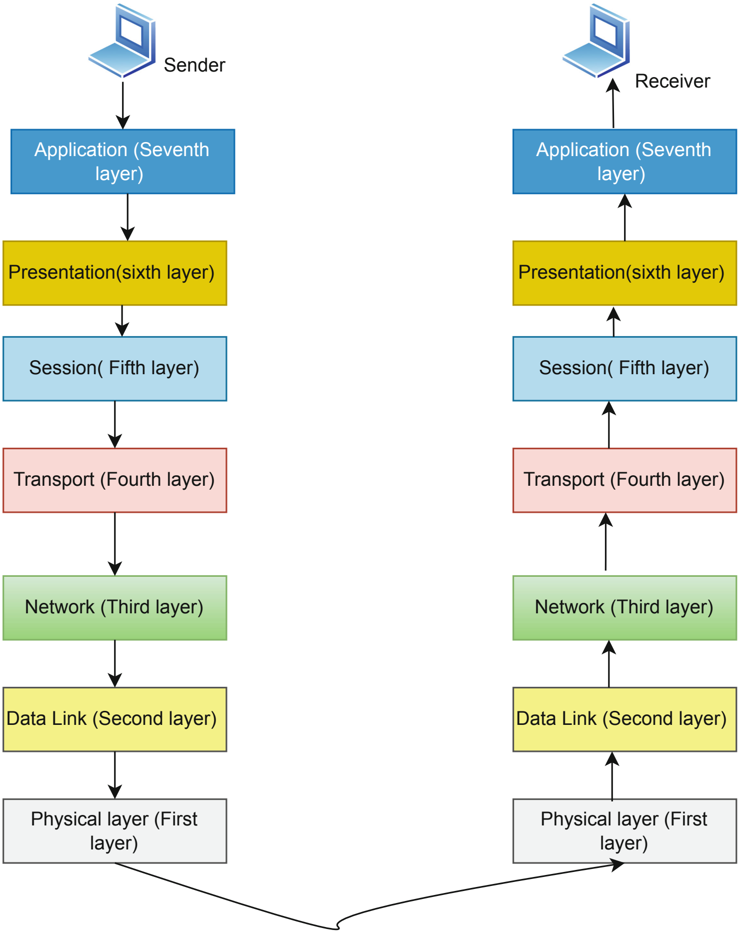


Fig. 1. OSI Reference Model Diagram

Smurf Attack. This category of attack takes advantage of the vulnerability of the Internet Group Management Protocol (IGMP), Sending ICMP echo requests to all devices in the network, rather than a specific device, causing all hosts on the network to respond to the target system.

2.2 Attack Methods and Strategies

Network layer DoS attacks can be launched using various attack methods and strategies, including the following (Fig. 2)

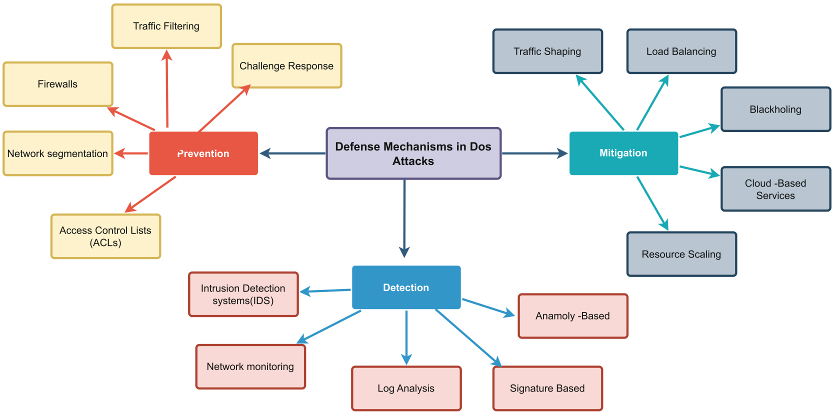


Fig. 2. Defense mechanisms in Dos attacks

Flood Attacks. In this method, the attacker inundates the target system with an enormous quantity of packets, requests, or connections. to consume the network resources and cause the system to crash or freeze

DDoS Attacks. In this method, the attacker uses a network of compromised computers, known as a botnet, to initiate a synchronized attack on the intended systemic.

Amplification Attacks. This method exploits the vulnerability of certain network protocols, such as DNS, NTP, or SNMP, to generate a large volume of traffic that can overwhelm the target system.

2.3 Impact and Consequences of Attacks

Network layer DoS attacks can have severe impact and consequences on the intended system and network infrastructure. Some of the typical outcomes of such attacks comprise

Degraded Network Performance. The network traffic generated by the attack can cause congestion, packet loss, and delay, resulting in degraded network performance.

Service Disruption. The attack can disrupt the availability of network services, making it difficult or impossible for legitimate users to access them.

Corruption. The attack can cause data loss or corruption if the target system crashes or becomes unavailable during the attack.

3 Machine Learning Approaches

The utilization of Machine Learning (ML) approaches has become increasingly popular in the detection DoS attacks in network layer because of its capacity to evaluate volumes of data in real-time. For DoS detection, several machine learning (ML) techniques have been suggested, including supervised, unsupervised, reinforcement, and hybrid learning (Fig. 3).

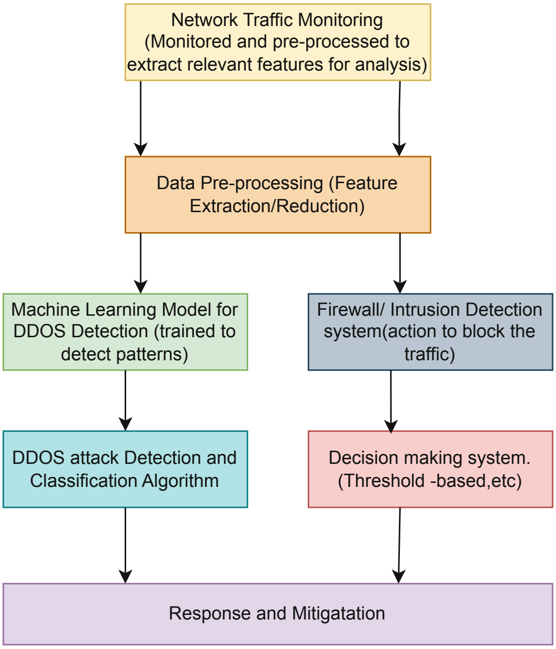

Network Traffic Monitoring (Monitored and pre-processed to extract relevant features for analysis)
Data Pre-processing (Feature Extraction/Reduction)
Machine Learning Model for DDOS Detection (trained to detect patterns)
Firewall/ Intrusion Detection system(action to block the traffic)
DDOS attack Detection and Classification Algorithm
Decision making system. (Threshold -based,etc)
Response and Mitigatation

Fig. 3. Machine learning implementation

Approaches in deep learning can automatically learn features from raw network traffic data. Such type of approach includes CNNs and RNNs. Hybrid approaches combine multiple ML methods to enhance precision in detection and lower the occurrence of false positives. Some examples of hybrid approaches include combining supervised and unsupervised learning, using ensemble methods, or combining ML with rule-based methods. By utilizing labeled data, supervised learning Concepts can build a model makes separation between genuine and malicious network traffic. decision trees and support vector machines play vital role. Unsupervised learning methods, such clustering and anomaly detection, could detect patterns and outliers in network traffic without the need for labeled data. Q-learning and deep Q-networks (DQNs) are examples of reinforcement learning algorithms that train themselves to make decisions depending on input from their surroundings. There are approaches that can be employed to detect network traffic anomalies automatically. For instance, RNNs and CNNs can automatically learn features from unprocessed network traffic data. Hybrid methods, which use a combination of multiple algorithms dealing with ML, which has the potential to enhance detection precision and lower the occurrence of false positive results. Hybrid approaches can be created by combining ensemble methods, rule-based methods, and both supervised and unsupervised learning.

4 The Machine Learning Techniques

The use of ML has gained popularity in preventing and mitigating the effects of DoS attacks by several orders of magnitude. ML approaches enable network administrators to detect and react to DoS attacks in real-time by doing analysis on patterns and behaviors in network traffic. Previous research has explored the utility of the use of ML for DoS attack prevention, including both attack mitigation techniques and defense mechanisms. For instance, A robust approach to identify Denial of Service (DoS) attacks employing an auto-encoder based on Support Vector Machines (SVM). The authors have tested the proposed method on the CICIDS dataset and achieved an accuracy of 99.32% for detecting DoS attacks [9]. SVM approach was initially proposed which has gained significant attention in ML research due to its excellent results. Through supervised learning methods, SVM can carry out both classification and regression tasks [10]. Subsequently, a dataset is formed, consisting of DDoS attacks, and is then employed to identify and detect these attacks using an advanced version of support vector machines (ESVM) [11]. Later, a DDoS attack detection model was developed by combining SVM classification methods [12].

Moreover, A novel approach called CSBW-Random Forest has been introduced, which outperforms existing methods regarding the measures of recall, accuracy, F1-score, and precision. The proposed technique achieves a high rating of 0.997 and shows significantly improved performance in comparison to previous literature. Additionally, experiments demonstrate that the suggested model performs better than related works in reference to the rates of three types of predictions: incorrect positives, correct positives, and incorrect negatives. KNN assigns classes Using the principle of proximity as a basis. This is a type of sluggish learning model that necessitates less training time but more prediction time. Most classes in the k nearest data points are used to assign the class. The model can serve as both a classifier and a regressor, and the parameter K, which is a hyperparameter, can be adjusted to tune the model is easy to understand and implement but has disadvantages for instance, characteristics such as sensitivity to magnitude, high computational cost, and impracticality for handling large datasets [13].

In another study, feature selection techniques were employed to decrease the features from 41 to either 11 or 17, that includes LDA, PCS, RFE, and univariate feature selection. KNN was then used to classify the data, achieving an accuracy of 99.87% and 99.11% when using 17 and 11 features, respectively, with RFE. Similarly, an accuracy of 99.82% was achieved using PCA, and 99.79% using LDA and univariate feature selection techniques with 17 and 11 features [14].

Two studies investigated the effectiveness of the K Nearest Neighbors (KNN) algorithm on different datasets. The first study found that KNN achieved a ROC score of 0.985 on the WSN-DS type dataset. Furthermore, the second study evaluated KNN's performance on three datasets and found that it achieved a precision of 97.31% on the WSN-DS type dataset, 94.79% on the NSL-KDD type dataset, and 99.61% on the KDD-Cup99 type dataset [15].

A Bayesian network is a graphical model that utilizes probabilities in which a directed acyclic graph is used to illustrate the conditional relationships between variables. In wireless ad hoc network case, this approach can be applied to model network traffic behavior and identify unusual activity, including flooding-based denial-of-service attacks. The article outlines a technique that utilizes Bayesian inference to DoS attacks caused by SYN flooding in wireless ad hoc networks. Shifting towards the initial First part of the article, Bayesian inference is used to model the SYN traffic within the network statistically. This approach involves constructing a Bayesian network that considers the pertinent variables for SYN traffic, such as the quantity of incoming SYN packets, outgoing SYN-ACK packets, and the time intervals between SYN packets [16].

The second part of the article shows that Bayesian inference is equivalent to exponential weighted moving average (EWMA) in the case of a single variable. This equivalence results in a more effective method for identifying SYN flooding attacks in wireless ad hoc networks. The method can defend against various types of flooding-based DoS attacks with high accuracy and low false detection rate. Therefore, Bayesian inference is effective in detecting and protecting against SYN flooding-based DoS attacks [16]. Moreover, another proposed method employs a two-layer model to enhance the detection of minority attacks. The method employs statistical analysis to choose features relevant to the less frequent attacks, and then uses a separate dataset to train a multi-classifier artificial neural network, resulting in enhanced detection accuracy. The technique achieved a detection accuracy of 99.34% for minority attacks [17].

Moreover, another proposed model deals with an application of machine learning techniques for identifying SYN flood attacks, utilizing a dataset acquired from ethio telecom network. Four classification algorithms, Naive Bayes, AdaBoost, J48, and Artificial Neural Network (ANN), were tested, and J48 was found to have better detection performance. The paper suggests exploring additional data mining methods and adopting a hybrid approach by integrating IDS and IPS to enhance network security [18].

In addition, some researchers have proposed using ML-based solutions for DoS attack prevention. They have presented two multi-party EdDSA [Edwards-curve Digital Signature Algorithm] Protocols designed for settings with partially trustworthy and untrustworthy participants. These aim to provide a secure method of maintaining a global state without the need for distributed hashing, possible for EdDSA-based blockchains. They have additionally expanded the malicious protocol to withstand DoS attacks by detecting corrupted parties in the event of execution interruptions.They tested their EdDSA protocols on Alibaba cloud servers and found that their protocol in the malicious setting is significantly quicker than recent threshold EdDSA protocols. The protocols possess characteristics that render them suitable for threshold wallets intended for EdDSA-based cryptocurrencies, including efficiency, identifiable abort, and high compatibility [19].

The proposed framework can reduce the workload of network administrators and enhance the efficiency of DoS attack prevention. Moreover, other studies have explored the use of ML-based defense mechanisms for DoS attack prevention. For example, LogDoS is a DDoS prevention system that relies on a unique process that utilizes GET messages and logging-relying filtering to establish inter-domain type routing. The system inserts GET messages at the ICN routers along the sender's path to eliminate packets that are not a reply to a preceding request. Combining NDN network and PID-based ICNs, this hybrid method generates a potent resolution for preventing data flooding attacks. LogDoS-enabled routers can filter packets and prevent them from causing flooding attacks. Overall, LogDoS is a powerful tool in preventing DDoS attacks and enhancing the security of ICN networks [5].

Overall, ML techniques hold great promise for preventing and mitigating DoS attacks at the network layer. Nevertheless, it is essential to emphasize that ML-based solutions also have their limitations and challenges, such as the need for large amounts of labeled training data and the potential for adversarial attacks. Future research should continue to explore and address these challenges to advance the development of effective ML-based solutions for DoS attack prevention.

5 Comparison of Machine Learning Approaches

The security and availability of computer networks are greatly endangered by Denial-of-Service (DoS) attacks. There are numerous methods suggested for detecting and preventing DoS attacks, including those that utilize machine learning techniques. The objective of this paper is to compare various machine learning-based techniques for detecting and preventing DoS attacks, as well as an assessment of the efficiency of machine learning techniques in combating network layer DoS attacks. This paper compares machine learning-based techniques for DoS attack detection and prevention, as well as their effectiveness in network layer DoS attack prevention. SVM and RF have high accuracy for detection, but with higher computational overhead. KNN and NN have lower overhead, but lower accuracy. ANN and RF are effective for preventing DoS attacks with low overhead and good scalability. SVM and RF have a higher detection rate for network layer DoS attacks, but with higher overhead. DT and NB have lower overhead but lower detection rate. Overall, machine learning-based approaches are effective in enhancing network security against DoS attacks.

6 Open Research Challenges and Future Directions

Current machine learning-based techniques for detecting and preventing network layer DoS attacks face challenges such as limited availability and diversity of high-quality training data, difficulty in detecting sophisticated attacks, high false-positive rates or low detection rates, and limited interpretability. To address these gaps, emerging research trends include developing more robust and adaptive models using deep learning techniques, exploring explainable and interpretable machine learning models, and investigating transfer learning and federated learning approaches. Opportunities for further research and development include creating large and diverse datasets, exploring ensemble learning methods, investigating adversarial training, and integrating machine learning-based techniques with other security mechanisms.

7 Conclusion

In conclusion, the paper provides a comprehensive survey of ML techniques for detecting and preventing network layer DoS Type attacks. The paper highlights the strengths and limitations of different machine learning-based approaches, including rule-based methods, statistical methods, and deep learning methods. The study emphasizes the need for more robust and adaptive machine learning models, which can better detect sophisticated attacks and reduce false-positive rates. The paper also identifies emerging research trends and future research directions, such as exploring explainable and interpretable models, exploring transfer learning and federated learning methodologies., and integrating ML techniques with other security mechanisms. Overall, the study contributes to the understanding of the most advanced techniques in machine learning-based techniques for detecting and preventing network layer DoS attacks and provides insights for future research in this area.

References

1. Tayyab, M., Belaton, B., Anbar, M.: ICMPv6-based DoS and DDoS attacks detection using machine learning techniques, open challenges, and blockchain applicability: a review. IEEE Access **8**, 170529–170547 (2020)

2. Xing, F., Wenye, W.: Understanding dynamic denial of service attacks in mobile ad hoc networks. In: MILCoM 2006–2006 IEEE Military Communications conference. IEEE (2006)
3. Verma, A., Saha, R., Kumar, N., Kumar, G., et al.: A detailed survey of denial of service for IoT and multimedia systems: past, present and futuristic development. Multimedia Tools Appl. **81**(14), 19879–19944 (2022). https://doi.org/10.1007/s11042-021-11859-z
4. Gebremariam, G.G., Panda, J., Indu, S.: Blockchain-based secure localization against malicious nodes in IoT-based wireless sensor networks using federated learning. Wireless Commun. Mobile Comput. **2023** (2023)
5. Kukreti, S., et al.: DDoS attack using SYN flooding: a case study. In: 2022 9th International Conference on Computing for Sustainable Global Development (INDIACom). IEEE (2022)
6. Patel, L., et al.: Machine learning methods in drug discovery. Molecules **25**(22), 5277 (2020)
7. Subbulakshmi, T., et al.: A unified approach for detection and prevention of DDoS attacks using enhanced support vector machines and filtering mechanisms. ICTACT J. Commun. Technol. **4**(2), 737–743 (2013)
8. Baarzi, A.F.: Efficient service deployment on public cloud: a cost, performance, and security perspective. The Pennsylvania State University (2021)
9. Allagi, S., Rachh, R., Anami, B.: A robust support vector machine based autoencoder for DoS attacks identification in computer networks. In: 2021 International Conference on Intelligent Technologies (CONIT). IEEE (2021)
10. Drucker, H., Donghui, W., Vapnik, V.N.: Support vector machines for spam categorization. IEEE Trans. Neural Networks **10**(5), 1048–1054 (1999)
11. Al Duwairi, B., et al.: LogDoS: a novel logging-based DDoS prevention mechanism in path identifier-based information centric networks. Comput. Secur. **99**, 102071 (2020)
12. Ye, J., et al.: A DDoS attack detection method based on SVM in software defined network. Secur. Commun Networks **2018** (2018)
13. Krishnan, D., Singh, S.: Cost-sensitive bootstrapped weighted random forest for DoS attack detection in wireless sensor networks. In: TENCON 2021–2021 IEEE Region 10 Conference (TENCON). IEEE (2021)
14. Pande, S., Khamparia, A., Gupta, D.: Feature selection and comparison of classification algorithms for wireless sensor networks. J. Ambient Intell. Humanized Comput. 1–13 (2021). https://doi.org/10.1007/s12652-021-03411-6
15. Singh, N., Virmani, D.: Computational method to prove efficacy of datasets. J. Inf. Optim. Sci. **42**(1), 211–233 (2021)
16. Nishanth, N., Mujeeb, A.: Modeling and detection of flooding-based denial-of-service attack in wireless ad hoc network using Bayesian inference. IEEE Syst. J. **15**(1), 17–26 (2020)
17. Shrivastava, U., Sharma, N.: Artificial neural network based dual layered predictive model for rare attack detection. In: 2020 International Conference on Computational Performance Evaluation (ComPE). IEEE (2020)
18. Mariam, W.B.W., Negash, Y.: Performance evaluation of machine learning algorithms for detection of SYN flood attack. In: 2021 IEEE AFRICON. IEEE (2021)
19. Feng, Q., Yang, K., Ma, M., He, D.: Efficient multi-party EdDSA signature with identifiable aborts and its applications to blockchain. IEEE Trans. Inf. Forensics Secur. **18**, 1937–1950 (2023). https://doi.org/10.1109/TIFS.2023.3256710
20. Gupta, B.B., Joshi, R.C., Misra, M.: Defending against distributed denial of service attacks: issues and challenges. Inf. Secur. J.: Global Perspect. **18**(5), 224–247 (2009)

Power Analysis Side-Channel Attacks on Same and Cross-Device Settings: A Survey of Machine Learning Techniques

Ashutosh Ghimire, Vishnu Vardhan Baligodugula, and Fathi Amsaad(✉)

Wright State University, Dayton, OH 45435, USA
{ghimire.18,baligodugula.2,fathi.amsaad}@wright.edu

Abstract. Systems that use secret keys or personal details are seriously at risk from side-channel attacks, especially if they rely on power analysis. Attackers can use unintentional sources like power consumption and electromagnetic waves to extract sensitive information. Recently, machine learning has become a promising approach for executing power side-channel attacks that are efficient and effective for single and cross-device environments. This paper reviews various machine learning-based power side-channel attacks, including feature extraction techniques, classification methods, and countermeasures. This survey investigates same-device and cross-device attacks that use multiple devices for training an artificial intelligence model for this purpose. It examines the strengths and limitations of various machine learning algorithms and suggests areas for future research to address challenges.

Keywords: Security · Artificial Intelligence · Attack · Power Traces · Cross-device

1 Introduction

The burgeoning of connected devices and the IOT ecosystem has resulted in an enormous increase in the amount of data created by these devices [13]. Unfortunately, this expansion has also presented attackers with new chances to exploit system weaknesses. Power side-channel attacks, for example, have arisen as a significant concern to the security of these devices. These attacks take advantage of unintended information leakage from a device, allowing an attacker to infer sensitive information about its operation by measuring its power consumption.

Power side-channel attacks can be particularly devastating because they can be performed remotely and without physical access to the target device. Moreover, traditional countermeasures, such as hardware or software-based protections, can be costly, impractical, or ineffective against these attacks. To address these challenges, researchers have turned to machine learning techniques to detect and prevent power side-channel attacks [15].

Published by Springer Nature Switzerland AG 2024
D. Puthal et al. (Eds.): IFIPIoT 2023, IFIP AICT 684, pp. 357–367, 2024.
https://doi.org/10.1007/978-3-031-45882-8_24

This paper aims to present a comprehensive survey of side-channel attacks built on machine learning, covering single and cross-device settings. Our analysis includes a detailed examination for the present situation-of-the-art in attack models, feature extraction, classification, and countermeasures. Our primary focus is on the challenges posed by cross-device attacks, where a single machine learning model is trained using data from multiple devices. We provide a critical review of the advantages and disadvantages of various machine learning approaches for side-channel attacks and identify possible paths for future studies to address the current challenges. Our goal is to create a valuable resource for researchers, practitioners, and policymakers interested in enhancing the security of connected devices (Fig. 1).

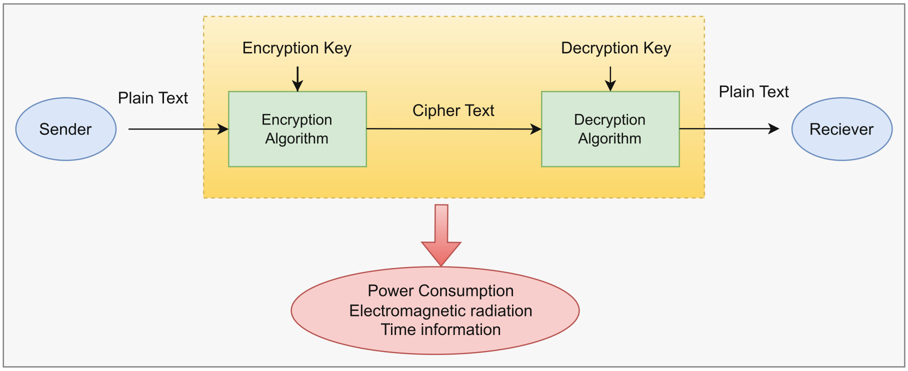


Fig. 1. Cryptosystems side channel information leakage

2 Background

2.1 Side-Channel Analysis (SCA)

Analyzing from the Side-Channel refers to various attacks that exploit unintended information leakage from a system's physical or implementation characteristics, such as electromagnetic radiation, timing information and power consumption. Such attacks can allow an attacker to obtain sensitive information about cryptographic keys or other secrets used within the system. Side-channel attacks can be categorized be determined by the type of side-channel signal used, including power analysis, electromagnetic analysis, acoustic analysis, and timing analysis.

Power Analysis (PA) is a sort of attack using side-channel information that analyzes the power usage of cryptographic equipment which can be divided into Differential Power Analysis (DPA) and Simple Power Analysis (SPA) [14]. Simple Power Analysis uses statistical analysis to directly examine the power usage of the devices in order to derive the secret key. This strategy needs a vast collection of data. In contrast, Differential Power Analysis compares power traces from different inputs to identify statistical differences that reveal the secret key. DPA is more advanced than SPA, but it also requires more expertise and complexity in analysis. It is crucial to understand the differences between these two techniques to effectively counteract power analysis attacks.

2.2 Machine Learning

An area in artificial intelligence called machine learning works on creating models capable of learning from data and making decisions or predictions without explicit programming. Several domains, including natural language processing, speech recognition, picture identification, and anomaly detection, have adopted this strategy [2,4].

In the realm of power side-channel attacks, researchers have proposed machine learning methods to increase the precision and effectiveness of attack detection and key recovery. These techniques can be categorized according to the type of learning algorithm used, such as supervised, unsupervised, and reinforcement learning.

2.3 Cross-Device Settings

Power side-channel attacks in cross-device settings refer to attacks that exploit side-channel information leaked by a device to extract the secret key used by another gadget in a different setting. This can happen when the same cryptographic key is used across multiple devices or when the side-channel information leaked by one device can be used to infer information about the key used by another device.

Cross-device attacks can be more challenging than attacks on a same-device because they involve dealing with different settings and conditions, such as different device architectures, operating systems, and environmental factors. Therefore, machine learning techniques that can handle cross-device variations and generalize well across different settings are particularly useful in this context.

3 Literature Review

Recent years have witnessed increasing interest in developing methods over side-channel attacks relying on machine learning and cross-device settings. Various survey papers have been published, outlining the latest state-of-the-art techniques in this field, and it is crucial to review and analyze their contributions.

In their survey paper published in 2019, Lee et al. provided an extensive review of the latest deep learning approaches utilized in side-channel attacks (SCA), which included CNNs and RNNs, and examined their strengths and limitations [11]. Additionally, they underscored the significance of further research and development in deep learning-based SCA techniques, particularly for their practical implementation.

Xu et al. (2021) proposed a method for cross-device attacks using unsupervised domain adaptation, which adapts the side-channel features extracted from a source device to a target device without requiring any labeled data from the target device [1]. The proposed technique shows significant improvement in attack performance compared to other existing methods.

Al-Ahmad et al. (2021) conducted a thorough review of power side-channel attacks, including their classifications, and the countermeasures designed to prevent them [16]. In their paper, the authors also discussed the challenges that hinder the progress of effective counter measures in case of these attacks.

In a separate study, Liu et al. (2021) proposed a novel method for stealing machine learning model parameters by taking advantage of the power consumption during model inference [21]. The proposed attack approach is capable of extracting sensitive information, such as the model weights and biases, which can be exploited to replicate the machine learning model and conduct further attacks.

This survey paper specifically focuses on cross-device settings for power side-channel attacks and explores the latent of artificial intelligence techniques in this area. We analyze the advantages and limitations of existing research and discuss the future directions of this field. Our paper aims to provide a more comprehensive understanding of the challenges and opportunities in cross-device power analysis side channel machine learning attack. It can serve as a useful reference for researchers and practitioners interested in understanding the latest developments and future directions in this field.

4 Machine Learning Approaches for Side Channel Analysis

SCA aim to obtain confidential information by exploiting the physical characteristics of a system, such as electromagnetic radiation or power consumption. In recent years, machine learning techniques have become a potent tool for improving the efficiency and efficacy of these assaults. This section will explore the latest advancements in machine learning based approaches for side-channel attacks, with a particular focus on two distinct settings: the same-device setting and the cross-device setting.

4.1 Same Device Setting

In the same-device setting, an attacker can obtain access to a same-device and monitor its side-channel emissions to extract confidential information. Recent advances in machine learning techniques have demonstrated encouraging outcomes in enhancing the efficiency and efficacy of side-channel attacks in this setting.

Convolution Neural Network. The use of Convolutional neural networks (CNNs) have gained increasing popularity in side-channel analysis to identify patterns in side-channel traces. Numerous studies have examined the potential of CNNs in exploiting information leakage from physical implementations of cryptographic systems such as AES, DES, and SHA. For instance, the paper [18] proposed a deep learning-based SCA approach using a CNN model for AES-128 with a single power consumption trace. Similarly, [12] suggested a 2D deep learning architecture for exploiting side-channel leakage in lattice-based key-exchange, whereas [24] introduced a multilabel deep learning-based SCA technique using a CNN model for AES-128 with a single power trace. These studies highlight the potential of CNNs in SCA for same-device settings and provide valuable perceptions by means of deep learning method in SCA.

LSTM. A study proposes a novel side-channel attack technique that uses a deep learning architecture cleaning-based STM and fully connected layers to predict secret key bits of an FPGA-based AES implementation [20]. The proposed attack technique is evaluated using two different types of attacks, SPA and DPA, and achieves a high success rate of 91.84% and 91.39%, respectively, outperforming existing side-channel attacks. The study uses power traces collected from an FPGA-based AES implementation, and the threat model assumes an attacker with access to these power traces.

DNNs. DNNs are widely used in side-channel analysis to extract sensitive information from cryptographic implementations. A novel side-channel attack technique is proposed in [10] that involves decomposing power traces into a linear combination of basis functions and subsequently using a DNN architecture to predict the secret key bits. The proposed method achieves high accuracy in predicting secret key bits and outperforms existing SCAs on AES and PRESENT implementations. The study uses power traces collected from cryptographic implementations, and the threat model assumes an attacker with access to these power traces.

Federated Learning. A federated learning-based side-channel attack technique is suggest in [19] to extract secret keys from devices while maintaining data privacy. The method involves training models on local datasets and aggregating the models' parameters on a server without disclosing any local information. The authors evaluate their approach on a smart card and demonstrate the effectiveness of the federated learning approach in extracting secret keys with improved accuracy while ensuring data privacy.

SVM. Support Vector Machines (SVMs) have gained popularity in side-channel analysis as a machine learning technique. In a recent study, the authors proposed a new attack method that utilizes SVMs to extract secret keys from cryptographic devices by analyzing the power consumption [7]. Their method involves training SVMs on power traces and using them to classify the power consumption patterns associated with different secret key values. Authors successfully demonstrated the vulnerability of cryptographic devices by precisely extracting the secret key from a smart card implementation of the AES cipher.

4.2 Cross-Device Setting

In the cross-device setting, the attacker has access to multiple devices and can use side-channel information from one device to attack another device with a similar implementation. Recent machine learning techniques have shown promise in improving the effectiveness of cross-device SCAs.

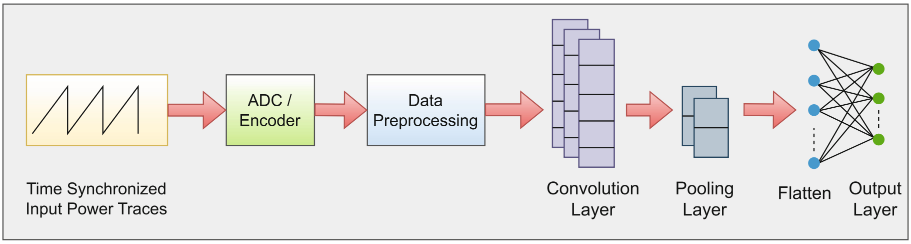


Fig. 2. Generic CNN training process for evaluating attack efficiency using power trace analysis.

CNN. CNNs are widely used in SCA to identify patterns in side-channel traces by capturing spatial dependencies between measurements. They have been applied to exploit information leakage from physical implementations of cryptographic systems, such as AES, DES, and SHA. Recent advances in deep learning-based SCA have been discussed in [3], along with their advantages and limitations. Another recent paper [9] proposes a CNN-based architecture using cross-subkey leakage that outperforms other methods on a new dataset. Figure 2 shows the generic example of training the CNN to assess the attack's effectiveness. The paper highlights the importance of considering cross-subkey leakage in side-channel analysis and provides a new avenue for developing deep learning-based techniques for practical implementation.

Autoencoder. Autoencoders are used in side-channel analysis as an unsupervised deep learning technique. In [5], The authors suggest a cross-device power side-channel attack using autoencoders. Their autoencoder-based attack model outperforms traditional methods in terms of success rate and accuracy, and they emphasize the importance of practical considerations such as low-cost sensors and real-time performance. In [23], the authors propose a denoising method called Noise2Clean using an unsupervised deep learning approach based on autoencoders. The proposed method is effective in denoising side-channel traces without using any prior knowledge of the noise model. The authors compare their results with other denoising methods and show that their method outperforms them in terms of denoising performance on two different datasets.

Transfer Learning. Transfer learning has become a popular technique in deep learning-based side-channel analysis, where pre-trained models on large datasets are leveraged to improve performance on smaller datasets. For instance, a study proposed a cross-device profiled SCA adapting pre-trained models for different devices utilizing the meta-transfer learning, and achieving better performance with fewer samples [22]. The authors evaluated their method on datasets including AES, DES, and SHA-3. Authors demonstrated an advanced side-channel attack using transfer learning and deep learning-based cross-family profiling that outperforms traditional and other deep learning-based methods [17]. They evaluated their method on datasets including AES and PRESENT and suggested that it enhances the transferability of deep learning-based SCA techniques across different cryptographic algorithms.

PCA. In SCA, feature analysis method like Principle Component Analysis is a widely used for reducing the dimensionality of data. Recently, researchers conducted a study where they successfully applied PCA to perform a side-channel attack on a software performance of AES-128. The study described the trial design and outcomes, emphasizing how the use of PCA significantly improved the attack success rate by reducing the dimensionality of power traces [8]. However, the paper also acknowledged the limitations of PCA and recommended exploring alternative dimensionality reduction techniques for side-channel analysis. Overall, this research highlights the potential of PCA in side-channel attacks and encourages further investigation into other methods to enhance the security of cryptographic implementations.

Support Vector Machine and Random Forest Classifier. SVM and random forest are two popular machine learning approaches in the area of side-channel analysis. A current study [6] investigates the suitability of these algorithms for multi-device profiling side-channel attacks, taking into account factors such as No of profiling traces, number of gadgets in the training set, and type of leakage model. The findings suggest that random forest performs better than SVM, especially when the number of profiling traces is small. This research provides valuable insights from the effectiveness of machine learning approaches to multi-device profiling side-channel attacks, aiding the selection of appropriate algorithms for such scenarios.

5 Strength and Limitations

In recent years, machine learning techniques have shown increased accuracy and efficiency in power side-channel attacks across different devices and architec-

Table 1. Table showing summary of the techniques

Machine Learning Approach	Strengths	Limitations	Paper/s
CNN	Able to learn complex features from raw power traces; good performance in cross-device and same-device scenarios	Requires large amounts of data and computational resources; vulnerable to overfitting	[3,9,12,18,24]
Autoencoder	Able to extract useful features and denoise power traces; practical and efficient for cross-device attacks	Limited to simple attack scenarios; requires manual selection of hyperparameters	[5,23]
Transfer Learning	Effective for transferring knowledge between different devices and attack scenarios; reduces the amount of required training data	Limited to similar devices or attacks; requires careful selection of transfer learning strategy	[17,22]
PCA	Simple and efficient; effective in same-device attacks	Limited to simple attack scenarios and linear correlations	[8]
SVM and Random Forest	Effective in multi-device profiling attacks; computationally efficient	Limited to linear correlations and simple attack scenarios	[6,7]
LSTM	Able to capture temporal dependencies in power traces; effective in same-device attacks	Requires careful tuning of hyperparameters; limited to simple attack scenarios	[20]
DNN	Able to simulate intricate non-linear connections between power traces and secret keys; effective in multi-device attacks	Requires large amounts of data and computational resources; vulnerable to overfitting	[10]
Federated Learning	Protects privacy of individual devices; reduces communication overhead	Limited to similar devices and attacks; requires careful selection of aggregation strategy	[19]

tures, making them a versatile tool in this field. However, limitations such as the requirement for large amounts of training data and the variability of targeted devices can limit their effectiveness. Despite these challenges, machine learning approaches are a promising area of research for power side-channel attacks, and are expected to continue playing an important role in the future.

Table 1 discuss briefly the strengths and limitations of different machine learning approaches for side-channel attacks in both same device and cross-device settings.

6 Future Research Directions for Overcoming Current Challenges

Despite the progress made in machine learning techniques for side-channel attacks, there are still several challenges that need to be addressed. Here are some potential research directions to overcome these challenges:

Robustness Against Adversarial Attacks: While adversarial machine learning techniques have been explored, there is still a need for more robust techniques that can resist sophisticated attacks. One potential direction is to combine multiple defense mechanisms, such as adversarial training, data augmentation, and model compression, to achieve greater robustness.

Generalization to New Devices: Transfer learning and meta learning techniques have shown promise in improving the generalization of side-channel attacks to new devices. However, these techniques still have limitations in scenarios where the devices are significantly different. Future research can explore novel techniques for transferring knowledge across different devices with varying implementations.

Privacy-Preserving Techniques: Federated learning is a promising technique for side-channel attacks while preserving the privacy of individual devices. However, it still requires a large amount of communication between devices, which can be a bottleneck in some scenarios. Future research can explore new techniques for privacy-preserving side-channel attacks that minimize the amount of communication required between devices.

Real-time Side-Channel Attacks: Several machine learning approaches uses in side-channel attacks involve offline training and testing, which may not be practical for real-time scenarios. To address this, future research could explore new approaches for conducting side-channel attacks in real-time, such as online learning and incremental learning. These techniques have the potential to enable real-time side-channel attacks with improved accuracy and efficiency, and could open up new avenues for applications in areas such as embedded systems and internet-of-things devices.

Side-Channel Attacks on Other Cryptographic Algorithms: While much of the existing research on machine learning approaches for side-channel attacks has centered on the AES algorithm, there is a growing need for methods that is applicable to different cryptographic methods as well. To address this, future research could investigate new techniques for conducting side-channel attacks on algorithms such as RSA and Elliptic Curve Cryptography. By expanding the scope of these techniques, researchers can push the boundaries of what is possible in this field and address the challenges associated with attacking a wider range of cryptographic systems.

Overall, these research directions have the potential to advance the recent techniques to enhance the effectiveness of machine learning techniques for SCA.

7 Conclusion

In conclusion, this survey paper has explored the use of machine learning approaches uses power side-channel attacks in cross-device settings. We began by discussing the basics of side-channel attacks and their relevance in modern-day security, followed by a review of recent research efforts in this field, categorized by the machine learning techniques used and the device settings in which they were tested.

Based on our analysis, we identified several key advantages of these approaches, including the ability to successfully extract secret information from multiple devices with high accuracy, the potential for real-world applications, and the efficiency and versatility of the machine learning techniques. However, there are also several limitations, such as the reliance on quality and quantity of training data, ethical and legal concerns, and the need for further research into generalizability and countermeasures.

Looking ahead, we believe that future research in this area should focus on addressing these limitations and further exploring the latent of machine learning approaches for power SCAs in cross-device settings. This includes developing more robust training data, exploring more ethical and legal ways to conduct experiments, and identifying more effective countermeasures to mitigate the risks of these types of attacks. While deep learning approaches, such as Autoencoder, CNN, and LSTM, show great promise for SCA applications, the presentation of the machine learning approach rely on the specific application and the characteristics of the target device. Therefore, the selection of machine learning approach needs to be carefully considered due to the context of the specific use case. By continuing to explore these avenues, we believe that this field can have a significant impact on improving the security of modern-day devices and systems.

References

1. Cao, P., Zhang, C., Lu, X., Gu, D.: Cross-device profiled side-channel attack with unsupervised domain adaptation. IACR Trans. Cryptograph. Hardw. Embed. Syst. 27–56 (2021)
2. Chapagain, A., Ghimire, A., Joshi, A., Jaiswal, A.: Predicting breast cancer using support vector machine learning algorithm. Int. Res. J. Innov. Eng. Technol. **4**(5), 10 (2020)
3. Das, D., Golder, A., Danial, J., Ghosh, S., Raychowdhury, A., Sen, S.: X-deepSCA: cross-device deep learning side channel attack. In: Proceedings of the 56th Annual Design Automation Conference 2019, pp. 1–6 (2019)
4. Ghimire, A., Tayara, H., Xuan, Z., Chong, K.T.: CSATDTA: prediction of drug-target binding affinity using convolution model with self-attention. Int. J. Mol. Sci. **23**(15), 8453 (2022)
5. Golder, A., Das, D., Danial, J., Ghosh, S., Sen, S., Raychowdhury, A.: Practical approaches toward deep-learning-based cross-device power side-channel attack. IEEE Trans. Very Large Scale Integr. (VLSI) Syst. **27**(12), 2720–2733 (2019)
6. Hanley, N., O'Neill, M., Tunstall, M., Marnane, W.P.: Empirical evaluation of multi-device profiling side-channel attacks. In: 2014 IEEE Workshop on Signal Processing Systems (SiPS), pp. 1–6. IEEE (2014)
7. Heuser, A., Zohner, M.: Intelligent machine homicide. In: Schindler, W., Huss, S.A. (eds.) COSADE 2012. LNCS, vol. 7275, pp. 249–264. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-29912-4_18

8. Hu, F., Ni, F.: Software implementation of AES-128: side channel attacks based on power traces decomposition. In: 2022 International Conference on Cyber Warfare and Security (ICCWS), pp. 14–21. IEEE (2022)
9. Hu, F., Wang, H., Wang, J.: Cross-subkey deep-learning side-channel analysis. IACR Cryptology ePrint Archive 2021, 1328 (2021)
10. Hu, F., Wang, H., Wang, J.: Side-channel attacks based on power trace decomposition. Cryptology ePrint Archive (2022)
11. Jin, S., Kim, S., Kim, H., Hong, S.: Recent advances in deep learning-based side-channel analysis. ETRI J. **42**(2), 292–304 (2020)
12. Kashyap, P., Aydin, F., Potluri, S., Franzon, P.D., Aysu, A.: 2Deep: enhancing side-channel attacks on lattice-based key-exchange via 2-D deep learning. IEEE Trans. Comput. Aided Des. Integr. Circuits Syst. **40**(6), 1217–1229 (2020)
13. Koblah, D.S., et al.: A survey and perspective on artificial intelligence for security-aware electronic design automation. ACM Trans. Des. Autom. Electron. Syst. (TODAES) (2022)
14. Meshgi, H., Khazaee, M.E., Kasiri, B., Shahhoseini, H.S.: An efficient algorithm resistant to spa and DPA variants in ECC. In: 2008 1st IFIP Wireless Days, pp. 1–5. IEEE (2008)
15. Patranabis, S., Mukhopadhyay, D.: Fault Tolerant Architectures for Cryptography and Hardware Security. Springer, Singapore (2018). https://doi.org/10.1007/978-981-10-1387-4
16. Randolph, M., Diehl, W.: Power side-channel attack analysis: a review of 20 years of study for the layman. Cryptography **4**(2), 15 (2020)
17. Thapar, D., Alam, M., Mukhopadhyay, D.: Deep learning assisted cross-family profiled side-channel attacks using transfer learning. In: 2021 22nd International Symposium on Quality Electronic Design (ISQED), pp. 178–185. IEEE (2021)
18. Wang, H.: Side-channel analysis of AES based on deep learning (2019)
19. Wang, H., Dubrova, E.: Federated learning in side-channel analysis. In: Hong, D. (ed.) ICISC 2020. LNCS, vol. 12593, pp. 257–272. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-68890-5_14
20. Wang, H., Dubrova, E.: Tandem deep learning side-channel attack on FPGA implementation of AES. SN Comput. Sci. **2**, 1–12 (2021)
21. Wolf, S., Hu, H., Cooley, R., Borowczak, M.: Stealing machine learning parameters via side channel power attacks. In: 2021 IEEE Computer Society Annual Symposium on VLSI (ISVLSI), pp. 242–247. IEEE (2021)
22. Yu, H., Shan, H., Panoff, M., Jin, Y.: Cross-device profiled side-channel attacks using meta-transfer learning. In: 2021 58th ACM/IEEE Design Automation Conference (DAC), pp. 703–708. IEEE (2021)
23. Yu, H., et al.: Noise2clean: cross-device side-channel traces denoising with unsupervised deep learning. Electronics **12**(4), 1054 (2023)
24. Zhang, L., Xing, X., Fan, J., Wang, Z., Wang, S.: Multilabel deep learning-based side-channel attack. IEEE Trans. Comput. Aided Des. Integr. Circuits Syst. **40**(6), 1207–1216 (2020)

Research Demo Session (RDS)

Lite-Agro: Exploring Light-Duty Computing Platforms for IoAT-Edge AI in Plant Disease Identification

Catherine Dockendorf[1], Alakananda Mitra[2], Saraju P. Mohanty[1](✉), and Elias Kougianos[3]

[1] Department of Computer Science and Engineering, University of North Texas, Denton, USA
{catherine.dockendorf,saraju.mohanty}@unt.edu
[2] Nebraska Water Center, Institute of Agriculture and Natural Resource, University of Nebraska-Lincoln, Lincoln, USA
amitra6@unl.edu
[3] Department of Electrical Engineering, University of North Texas, Denton, USA
elias.kougianos@unt.edu

Abstract. The Lite-Agro study aims to deploy deep learning neural network models for pear disease identification through tree leaf image analysis on TinyML device. A case study on pear leaves is conducted with publicly available pear disease dataset. Quantitative comparisons are made between different datasets. *Lite-Agro* is a light-duty image computing detection solution that is tested for deployment on a microcontroller. The novelty of *Lite-Agro*, lies in the export of a lightweight TinyML, Tensorflow Lite model that is geared for low power applications on battery powered hardware. The goal is to find the best model that is custom selected for the application and achieves the highest accuracy. The study emphasizes finding a balance between size, accuracy and performance. In future iterations of the study, Lite-Agro is to be mounted on an unmanned aerial vehicle to be powered with solar panels. Modern low powered microcontroller devices are to be a staple implementation in Smart Villages.

Keywords: Smart Agriculture · Agriculture Cyber-Physical System (A-CPS) · Internet of Agro Things (IoAT) · Smart Village · TinyML · Edge-AI · Plant Health · Plant Disease

1 Introduction

Deep Learning has made major advancement in the last ten years. They are being employed in applications encompassing a wide range of use cases from speech generation, text processing and image identification. In 2020, the world wide yield of pear was 23 metric tons. However, pear diseases can adversely affect the pear yield. Early and automatic detection of pear diseases can stop over use of herbicides, reduce the cost related to the expensive expert services to detect the diseases, and mitigate the disease early to reduce the financial loss of the farmers.

Published by Springer Nature Switzerland AG 2024
D. Puthal et al. (Eds.): IFIPIoT 2023, IFIP AICT 684, pp. 371–380, 2024.
https://doi.org/10.1007/978-3-031-45882-8_25

When deep neural networks (DNN) are employed to detect plant diseases, they automatically extract the features from the input data and detect the disease. DNN provides high accuracy after training with a large dataset. Images of the pear leaves can be used as the input data. However, this current research, *Lite-Agro*, aims to bring the solution to the farmer with a low power edge solution. This research on TinyML [20] and it's application on micro controllers branches off from a plant disease identification [14] and crop damage estimation [15] study. *Lite-Agro*, applies deep learning to improve efficiency in Smart Agriculture [16]. *Lite-Agro* is designed to be a lightweight system that runs on a low power microcontroller and aims to find optimization in terms of model accuracy while being a low cost hardware implementation.

The paper is currently organized into various sections. Section 2 summarizes novel contribution. Section 3 discusses prior work. A system level overview is discussed in Sect. 4. Section 5 talks about proposed training methods and a comparative perspective. Experimental validation is discussed in Sect. 6. Section 7 concludes the article with an overview of future work.

2 Novel Contributions of the Current Paper

2.1 Problem Addressed and Proposed Solution

Lite-Agro, a lightweight, low power TinyML-based pear disease identification system, is proposed to address the needs of a plant disease solution in pear farms. Manual inspection of leaves for plant diseases translate to time inefficiencies. A combination of various deep learning models were trained until the best recognition accuracy was attained. The novelty lies in the application of compact modern Convolutional Neural Networks (CNNs) that are evaluated on a publicly available dataset [6]. The CNN-based model Xception generated the highest recognition accuracy of 99.97% however due to microcontroller memory constraints, other models are being considered. This is important as a computing gear for smart villages.

2.2 Novelty and Significance of Proposed Solution

The novelty of Lite-Agro lies in the exploration of low powered and lightweight hardware platform for the optimum TensorFlow [29] Lite model, trained to learn the identification of diseases in pear leaves. The study looks at how modern deep learning convolutional neural networks contribute to the optimization and reliability of TinyML [8] applications. The exploration of a light-duty computing hardware platforms powered by TinyML: TensorFlow Lite for microcontrollers has key potential in Smart Village edge devices. Exploring TinyML options and how it can be utilized as the hardware solution for a TinyML image capture implementation, comprises as the element of novelty in this study.

3 Related Prior Works

The work in [28] has explored three classifications of infections; *Septoria piricola* [1,25], *Alternaria alternate*, and *Gymnasporangium haracannum* [11]. DiAMOS plant study, mentions the use of pretrained models or an ensemble of pretrained models such as EfficientNetB0 [24], InceptionV3 [23], MobileNetV2 [19], and VGG19 [22]. To conclude with a model that results in the highest accuracy, the study employed training on the PDD2018 dataset with VGG16, InceptionV3, and Resnet50 [12] models. Data augmentation, number of epochs and image resolution size, were the variable parameters in the experiment. Table 1 presents a summary of these works.

Alternaria alternata in plant disease pathology, is defined as a type of an opportunistic fungus that is the cause of spot or discoloration on leaves. *Gymnosporangium haracannum* [11], more commonly called as juniper rusts, is an orange lesion and rust like spotting on a leaf. The disease is more of a cosmetic eyesore since infected fruits can look like corona gelatinous fingers. *Septoria pyricola* [1], is another plant disease found on Pears (Pyrus Communis). Outbreaks have been said to have occurred in pear orchards. A simple description of this disease is a brown outer rim leaf spot with a white central lesion.

Table 1. Accuracy of CNN and Ensemble-based Models in the PDD2018 *(left)* DiaMOS Study *(right)*.

PDD2018 Study	Accuracy	DiaMOS Study	Pixel Size	Accuracy
EfficientNetB0 [24]	89.02%	VGG16	224 × 224	78.34%
InceptionV3 [23]	84.44%	VGG16	600 × 600	96.80%
MobileNetV2 [19]	87.70%	InceptionV3	224 × 224	80.23%
EfficientNetB0 + InceptionV3	91.14%	InceptionV3	600 × 600	97.99%
EfficientNetB0 + MobileNetV2	86.21%	ResNet50	224 × 224	73.85%
InceptionV3 + MobileNetV2	85.35%	ResNet50	600 × 600	98.70%

The study conducted in [5] benchmarks a comparison between an ensemble combination of three neural networks such as EfficientNetB0 [24], MobileNetV2 [19], and InceptionV3 [23]. EfficientNetB0 + InceptionV3 [12], produced the highest value of recognition accuracy at 91.14%. CNN-based plant disease identification is presented in [13]. In [26], a study that incorporates the novel use of solar power in the hardware aspect of plant disease identification has been presented.

4 Lite-Agro: A System Level Overview

The system overview of Lite-Agro is shown in the Fig. 1. A public image dataset is used for the training of the model. In terms of software, the research utilizes Tensorflow [7], a framework written in Python that contains C++ machine learning [21] and artificial intelligence libraries. On top of that is Keras, which is defined as a software API

(Application Programming Interface), fully integrated with the backend TensorFlow. GPUs have revolutionized machine learning studies and have enabled researchers to explore and apply real time parallel processing algorithms. Using AMD's open source framework ROCm, the authors perform high performance computing experiments and maximize multi-core capabilities [17]. The model generated through Tiny ML techniques, is exported as a Tensorflow Lite model that is then converted as a C source code byte array. Tensorflow Lite is the ultra low power port of TensorFlow designed to run on microcontrollers [27]. The EspressIf firmware compiles the model and the program together. The lightweight TinyML model runs on a single-board computer, which interfaces with an edge-server board equipped with a camera.

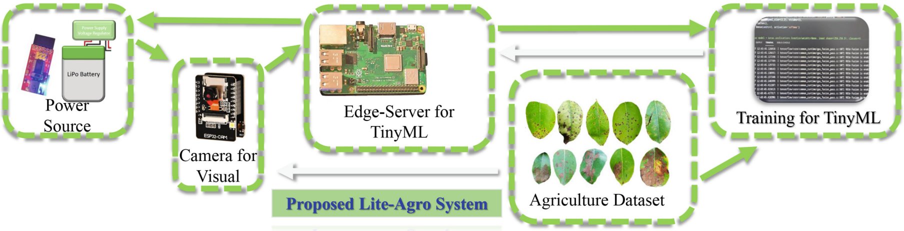


Fig. 1. System Overview of Lite-Agro.

5 Proposed Training Method

5.1 Proposed Methodology

The debate whether to train using deep learning and which platform to choose, is a critical question in the *Lite-Agro* study. Deep learning is preferred, and this is attributed to the accuracy of results. The prospect of the automated predictive capability offered by deep learning is a state of the art technology by itself, and the possibilities on the application of automation are endless. A CNN Network, the master algorithm in computer vision [18] is an imagery architecture used to process the pixels of images. Model Training is the step where a network learns from the dataset to determine's the model's weight and biases. A summary of the Tensorflow model training algorithm procedure used in this study is shown in Algorithm 1.

Algorithm 1. TensorFlowLite Model Training Procedure with Keras API.

```
Declare folder path and run Image Data Generator on training, validation and test labels.
for $iteration = 1, \ldots, 3006$ images do
    Preprocess images via VGG16.
    Call flow from directory and pass folder path, image size, classes and batch size.
    Preprocess image dataset from directory.
    Set parameters categorical cross-entropy and $256 \times 256$ image size.
    Set color mode RGB, batch size, and validation split of 0.2.
end for
for $iteration = 1, \ldots, 3006$ images do
    Preprocess image validation set from directory with categorical $256 \times 256$ image size.
    Set color mode RGB, batch size and validation split of 0.2.
end for
Declare a Sequential Model or call a Pretrained model.
Compile with rmsprop, categorical cross entropy, and set accuracy metrics.
for $iteration = 1, \ldots, 100$ epochs do
    Train model by calling the fit method.
end for
Save Model and Weights. Load Model.
Convert Keras Model to TensorFlowLite Model. Open file to save.
```

Epoch was set to 100 and it took 6 h and 45 min to reach accuracy of 99.73%. The best performing model was produced by an InceptionV3 [23] inspired architecture,"Xception" [2] model. The Inception [23] model, is a stack of layers meant to extract features and are conceptually similar to convolutions, which are highly intensive computational processes. Keras libraries abstract the convolution process in it's library function calls. Various combinations of parameters were tested to generate the best accuracy numbers. The Xception architecture's performance is attributed to the more efficient use of model parameters. The Table 2 shows a comparative analysis between PDD2018, DiaMOS and the current paper (*Lite-Agro*). The approach was adopted in [5] to address the accuracy problem on pear disease recognition, was to adopt an ensemble CNN method during training.

Table 2. Quantitative Analysis of Current Paper with existing Pear Disease Imaging Works.

Works	Dataset	Resolution Size	Model	Recognition Accuracy
Yang, et al. [7]	PDD2018	600 × 600	Resnet50 [9]	98.7%
Fenu, et al. [3]	DiaMOS	224 × 224	EfficientNetB0 [24]+InceptionV3 [23]	91.14%
Current Paper (Lite-Agro)	DiaMOS	256 × 256	Xception [2]	99.73%

Compilation is the step to prepare the model for training. An optimizer is a learning algorithm that models the input and adjusts the network as it undergoes training. In previous paper studies [5], most mention Adam optimizer as the default choice. Adam optimizer is a learning algorithm characterized as an extension of a stochastic gradient. It is best suited for large datasets and calculates at random points in each iteration to achieve a faster convergence. In this experimentation, the compile step argument selected was an RMSprop optimizer. In an RMSprop optimizer, gradient descent algorithms, achieving a faster learning rate as steps increments are larger, leading to a faster convergence.

5.2 Evaluation Metrics

We see how recognition accuracy increases in every epoch stage throughout the training. Tensorboard handles the logging, reporting and graph generation. Data visualization becomes easier given the set of TensorFlow tools. The graph on Fig. 2 shows the trend of accuracy increase per epoch during the training procedure.

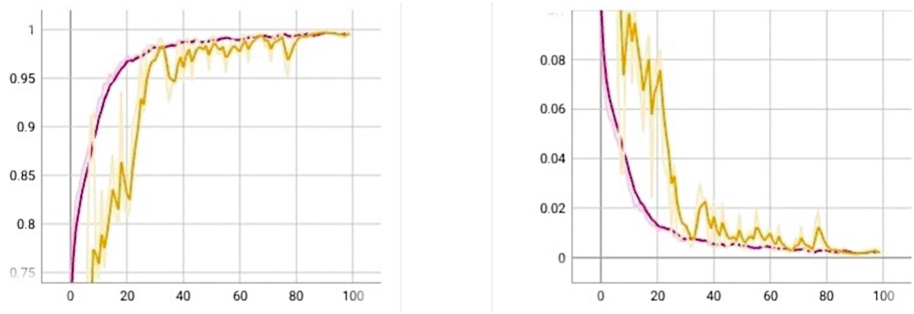
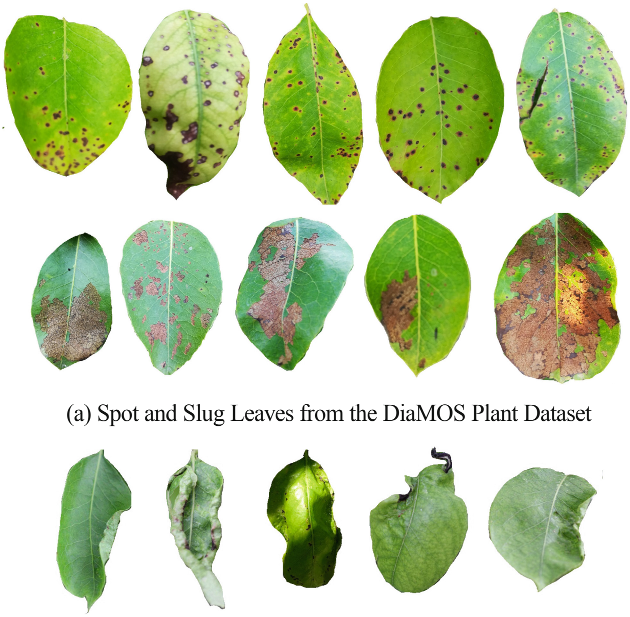


Fig. 2. Recognition Accuracy *(left)* vs Loss *(right)* at Various Epochs.

6 Experimental Results

We used DiaMOS dataset consisting of 3505 images of pear leaves of which fall under four classifications; healthy, spot, slug and curl [5]. A selected example is presented in Fig. 3.

TinyML [20], short for Tiny Machine Learning, describes hardware, algorithms, and software [27]. TinyML targets being able to run inference programs on battery operated hardware and memory constrained implementation. The ability to port ML models on microcontrollers brings about countless application possibilities. Much of the emphasis in this study will be on a TensorFlow version of TinyML called, TensorFlow Lite for Microcontrollers. Keras API allows the conversion of an .h5 format of a model into a compact TFLite extension. This TensorFlow Lite conversion allows bigger models with a relatively large size, to execute in a more compact form. An Xception trained model of size $163,373$ KB for example, when ran through the aforementioned TFLite converter, gets compacted down to $81,257$ KB. This port of TensorFlow is optimized for running on edge devices and geared for space efficiency and addresses memory constraints. The TFLite model is once again converted to a *C* source file byte array, that describes the model. Inference is then run on the trained model and translated



(a) Spot and Slug Leaves from the DiaMOS Plant Dataset

(b) Curled Leaves from the DiaMOS Plant Dataset

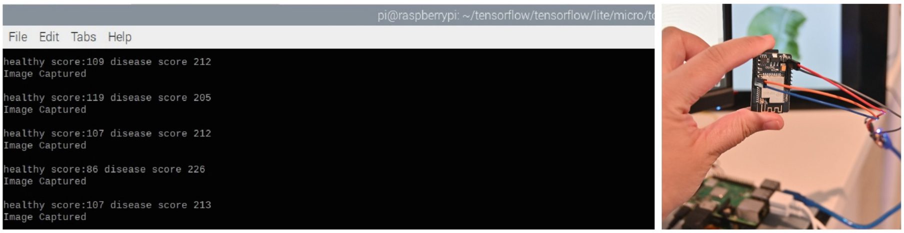
Fig. 3. Representative of the DiaMOS Plant Dataset.

into the most probable set of classification. Currently, there are a limited number of development boards supported by TFLM, mentioned on the TensorFlow website which are summarized in the Table 3.

Table 3. Comparison of Tensorflow Supported Platforms.

Board	Microprocessor	CPU Clock	Voltage	SRAM Size	Connectivity
Arduino Nano 33 BLE Sense	nRF52840	64 MHz	3.3 V	256 KB	USB UART, SPI, I2C, BLE, SPI
STM32F746 Discovery Kit	32bit ARM Cortex	48 MHz	3 V–5 V	192 KB	USB LQFP100 I/O
Espress ESP-EYE	32-bit ESP32	240 MHz	3.3 V	8 MB PSRAM	UARD, USB, BLE, SPI, I2C, WiFi
Sony Spresense	-M4F6 Core	156 MHz	3.3 V–5 V	1.5 MB	GNSS, UART, I2C, SPI, I2S

Onboard is the Xtensa single/dual core 32 bit LX6 microprocessor [30] with 448 KB ROM, 520 KB SRAM and 16 KB SRAM. To program the ESP32-CAM WiFi, TensorFlow Lite uses firmware EspressIDF [4] to build and configure the board. Lastly, once the source code has been modified, the trained model is added, then the program can once again be flashed from the Raspberry Pi 3B board to the SD card and executed using a monitor call. Initially, the ESP32-CAM GPIO pins are interfaced with FTDI adapter. With the ESP32-CAM wiring set-up, the main complication lies in the need to connect the GPIO0 to ground every time the program needs to be reflashed. The ESP32-CAM takes photos at specific intervals and displays information whether the pear leaf is healthy or not through a monitor. Once it detects a diseased pear leaf, the information shall be displayed to an edge server and peripherals may be connected to display the information (Fig. 4).



```
healthy score:109 disease score 212
Image Captured

healthy score:119 disease score 205
Image Captured

healthy score:107 disease score 212
Image Captured

healthy score:86 disease score 226
Image Captured

healthy score:107 disease score 213
Image Captured
```

Fig. 4. IDF Monitor Pear Disease Detection Test *(left)*. Test Set-up (*right*)

7 Conclusion and Future Work

Deployment of deep learning models trained in pear disease identification, implemented on micro controllers were explored. A lightweight port of Tensorflow called TinyML [27] or TensorFlow Lite was used. The ESP32-CAM delivers a balance of price, power and performance and make a good hardware selection for edge devices. Often times, memory is severely resource constrained [3] but being able to run tiny deep learning models have great contribution in the automation of devices. This is why light-duty computing platform for IoAT-Edge devices and how it can improve the processing in Smart Agriculture processes was explored. The deployment of Lite-Agro in a proper testing environment where the pears are located and being able to gather actual field data can further contribute to this study. Researchers can further verify whether the models deliver the performance that the recognition accuracy numbers claim to deliver. The possibility of adding a battery or solar component and mounting on an unmanned aerial vehicle [10] would be an interesting future work expansion.

References

1. Chatzidimopoulos, M., Pappas, A.: Epidemiology and control of Septoria pyricola in pear leaf and fruit. J. Plant Pathol. **98**, 447–452 (2016). https://doi.org/10.4454/JPP.V98I3.020
2. Chollet, F.: Xception: deep learning with depthwise separable convolutions (2017). https://doi.org/10.1109/cvpr.2017.195
3. David, R., et al.: TensorFlow lite micro: embedded machine learning on TinyML systems. CoRR abs/2010.08678 (2020). https://arxiv.org/abs/2010.08678
4. Espressif Systems: EspressIDF: IoT Development Framework. https://docs.espressif.com/projects/esp-idf/en/latest/esp32/get-started/linux-macos-setup.html. Accessed 8 May 2023

5. Fenu, G., Malloci, F.M.: Classification of pear leaf diseases based on ensemble convolutional neural networks. AgriEngineering **5**, 141–152 (2023). https://doi.org/10.3390/agriengineering5010009
6. Fenu, G., Malloci, F.M.: DiaMOS plant: a dataset for diagnosis and monitoring plant disease. Agronomy **11**, 2107 (2021). https://doi.org/10.3390/agronomy11112107
7. Google Inc.: TensorFlow: large-scale machine learning on heterogeneous systems. https://www.tensorflow.org/. Accessed 8 May 2023
8. Han, H., Siebert, J.: TinyML: a systematic review and synthesis of existing research (2022). https://doi.org/10.1109/icaiic54071.2022.9722636
9. He, K., Zhang, X., Ren, S., Sun, J.: Deep residual learning for image recognition. In: Proceedings of IEEE Conference on Computer Vision and Pattern Recognition (CVPR), pp. 770–778, June 2016. https://doi.org/10.1109/CVPR.2016.90
10. Karar, M.E., Alotaibi, F., Al-Rasheed, A., Reyad, O.: A pilot study of smart agricultural irrigation using Unmanned Aerial Vehicles and IoT-Based Cloud System. Inf. Sci. Lett. **10**, 131–140 (2021). https://doi.org/10.18576/isl/100115
11. Lāce, B.: Gymnosporangium species - an important issue of plant protection. Proc. Latvian Acad. Sci. Sect. B. Nat. Exact Appl. Sci. **71**, 95–102 (2017). https://doi.org/10.1515/prolas-2017-0017
12. Mathworks Inc.: Pretrained deep neural networks. https://www.mathworks.com/help/deeplearning/ug/pretrained-convolutional-neural-networks.html. Accessed 8 May 2023
13. Mitra, A., Mohanty, S.P., Kougianos, E.: A smart agriculture framework to automatically track the spread of plant diseases using mask region-based convolutional neural network. In: Proceedings of the 5th IFIP International Internet of Things Conference (IFIP-IoT), pp. 68–85 (2022). https://doi.org/10.1007/978-3-031-18872-5_5
14. Mitra, A., Mohanty, S.P., Kougianos, E.: aGROdet: a novel framework for plant disease detection and leaf damage estimation. In: Proceedings of the 5th IFIP International Internet of Things Conference (IFIP-IoT), pp. 3–22 (2022). https://doi.org/10.1007/978-3-031-18872-5_1
15. Mitra, A., Singhal, A., Mohanty, S.P., Kougianos, E., Ray, C.: eCrop: a novel framework for automatic crop damage estimation in smart agriculture. SN Comput. Sci. **3**(4), 16 (2022). https://doi.org/10.1007/s42979-022-01216-8
16. Mitra, A., et al.: Everything you wanted to know about smart agriculture. CoRR abs/2201.04754 (2022). https://arxiv.org/abs/2201.04754
17. Rehman, Z.U., et al.: Recognizing apple leaf diseases using a novel parallel real-time processing framework based on mask RCNN and transfer learning: an application for smart agriculture. IET Image Process. **15**, 2157–2168 (2021). https://doi.org/10.1049/ipr2.12183
18. Russakovsky, O., et al.: ImageNet large scale visual recognition challenge (2015)
19. Sandler, M., Howard, A., Zhu, M., Zhmoginov, A., Chen, L.C.: MobileNetV2: inverted residuals and linear bottlenecks (2018). https://doi.org/10.1109/cvpr.2018.00474
20. Schizas, N., Karras, A., Karras, C., Sioutas, S.: TinyML for ultra-low power AI and large scale IoT deployments: a systematic review. Future Internet **14**, 363 (2022). https://doi.org/10.3390/fi14120363
21. Silaparasetty, N.: Machine learning programming with TensorFlow 2.0 (2020). https://doi.org/10.1007/978-1-4842-5967-2_11
22. Simonyan, K., Zisserman, A.: Very deep convolutional networks for large-scale image recognition. In: Bengio, Y., LeCun, Y. (eds.) 3rd International Conference on Learning Representations, ICLR 2015, San Diego, CA, USA, 7–9 May 2015, Conference Track Proceedings (2015). http://arxiv.org/abs/1409.1556
23. Szegedy, C., Vanhoucke, V., Ioffe, S., Shlens, J., Wojna, Z.: Rethinking the inception architecture for computer vision (2016). https://doi.org/10.1109/cvpr.2016.308

24. Tan, M., Le, Q.V.: EfficientNet: rethinking model scaling for convolutional neural networks. In: Proceedings of the 36th International Conference on Machine Learning, pp. 6105–6114 (2019)
25. Thomidis, T., Katerinis, S.: Occurrence of a fruit spot disease of pear caused by Septoria pyricola in Tyrnavos Larissa, Northern Greece. Plant Dis. **98**, 845–845 (2014). https://doi.org/10.1094/pdis-09-13-0960-pdn
26. Udutalapally, V., Mohanty, S.P., Pallagani, V., Khandelwal, V.: sCrop: a novel device for sustainable automatic disease prediction, crop selection, and irrigation in Internet-of-Agro-Things for smart. Agriculture **21**, 17525–17538 (2021). https://doi.org/10.1109/jsen.2020.3032438
27. Warden, P., Situnayake, D.: TinyML: Machine Learning with TensorFlowLite on Arduino and Ultra Low Power Microcontrollers. O'Reilly Media, Inc., London (2019)
28. Yang, F., Li, F., Zhang, K., Zhang, W., Li, S.: Influencing factors analysis in pear disease recognition using deep learning. Peer-to-Peer Networking Appl. **14**(3), 1816–1828 (2020). https://doi.org/10.1007/s12083-020-01041-x
29. Zaman, F.: TFLite architecture (2020). https://doi.org/10.1007/978-1-4842-6666-3_4
30. Ziaul Haque Zim, M.: TinyML: analysis of Xtensa LX6 microprocessor for neural network applications by ESP32 SoC. arXiv e-prints arXiv:2106.10652, June 2021. https://doi.org/10.48550/arXiv.2106.10652

FarmIns: Blockchain Leveraged Secure and Reliable Crop Insurance Management System

Musharraf Alruwaill[1], Anand Kumar Bapatla[1], Saraju P. Mohanty[1](✉), and Elias Kougianos[2]

[1] Department of Computer Science and Engineering, University of North Texas, Denton, USA
{MusharrafAlruwaill,anandkumarbapatla}@my.unt.edu, saraju.mohanty@unt.edu
[2] Department of Electrical Engineering, University of North Texas, Denton, USA
elias.kougianos@unt.edu

Abstract. Farmer uses traditional crop insurance to protect their farms against crop loss and natural risks. However, farmers are concerned about crop insurance claims due to delays in processing claims that cost significantly. Insurance fraud is another problem in crop insurance which costs significantly for insurance companies. The proposed FarmIns framework uses blockchain technology, allowing farmers to create and manage insurance agreements with insurance providers through smart contracts and creating a verifiable log of farm monitoring parameters to help insurance providers verify and approve claims promptly. FarmIns uses the Internet of Agro-Things (IoAT), and video surveillance technologies like Closed-Circuit Television (CCTV) to monitor and provide reliable farm data to process claims. FarmIns also acts as Decision Support Tool (DST) for both the insurer and the insured.

Keywords: Agriculture Cyber-Physical System (H-CPS) · Internet-of-Agro-Things (IoAT) · Blockchain · Smart Contract · Insurance Claim

1 Introduction

Agriculture is one of the important occupation for sustainable living and providing food safety for rapidly increasing population. With raise in population and increase in food demand, traditional farm techniques has been modernized by adapting latest technological advancements to make the farms more productive and use less resources [1,2].

Traditional insurance has several issues, such as fraudulent claims and the lack of transparency and complexity of the review process, which will take significant time and could negatively impact farmers. Therefore, the proposed framework, FarmIns, which is based on weather-based index insurance (WBII), addresses these issues, and solves them with the help of blockchain technology,

Published by Springer Nature Switzerland AG 2024
D. Puthal et al. (Eds.): IFIPIoT 2023, IFIP AICT 684, pp. 381–389, 2024.
https://doi.org/10.1007/978-3-031-45882-8_26

smart contracts, cloud computing, a decentralized oracle network, and the Internet of Agro-Things (IoAT). Smart contracts are used for creating and managing insurance policies between farmers and insurance companies along with providing a robust Role Based Access Control mechanism (RBAC). Cloud computing is used to create a decision support tool for the efficient management of the farm. Decentralized oracles are used to provide reliable data to the smart contracts for efficient verification of real-time farm parameters to process claims.

2 Related Prior Works

Different blockchain based solutions for farm insurance has been explored in this section. Neo drought has proposed NEO smart contract based irrigation monitoring system [1]. The proposed framework in [2], focusing on the gas fees optimization while relying on single API to make a decision. [3] presents a blockchain based crop insurance with smart contract that makes an agreement between the farmers and insurance company. At [4] uses blockchain Hyperledger Fabric for preventing false claim. At [5] the proposed system address several issues the farmer is facing such as middle man and transparency. [6] uses Proof of Authority (PoA) consensus algorithm to proof of capability of blockchain to be used in insurance sector as for different cases such as supply-chain and car insurance. At [7] proposed framework uses private blockchain network (Hyperledger Fabric) for insurance services with smart contract to automate insurance services in secure manner such as claim automation to reduce the claim process.

The proposed framework FarmIns has a different framework and design, as well as additional functionalities, to streamline the process between the insurer and the insured with security perspectives. It enables IoAT to monitor the farm and cloud to process and authenticate IoAT devices. FarmIns uses blockchain technology and smart contract to securely stores the data and automates the claim process and other insurance procedures. It also provides risk elimination with the aid of a notification system to minimize loss to the greatest extent possible. In addition, Chainlink is used to validate the data, provide an accurate value, and avoid reliance on a single data provider. At Table 1 presents the comparison of proposed system and other related works.

3 Novel Contributions of the Current Paper

3.1 The Problem Addressed

Traditional crop insurance has multiple of drawbacks which have a significant impact on the farmer, especially smallholder farmers.

Due to distributed nature of entities participating in the insurance management system creates lack of transparency and in turn causes processing delays. Most of today's systems are centralized which are prone to security threats and data manipulations. Hence, getting reliable data for insurance companies to process the claims is a problem. Along with these, false claims are another problem

Table 1. IoT and Access Management Related Work

Framework	IoT Integration	Access-Control Management	Real-Time DST	IoT Data Validation	IoT Data Reliability And Accuracy
Nguyen et al., 2019 [1]	No	No	Yes	NA	NA
Salem et al., 2021 [2]	No	No	Yes	No	Low
Jha et al., 2021 [3]	No	Yes	No	No	No
Gera et al., 2020 [4]	No	No	No	No	No
Patel and Shrimali, 2021 [5]	Yes	Assumption	No	No	No
Aleksieva et al., 2020 [7]	No	No	No	No	No
Khan et al., 2021 [6]	Yes	Yes	No	No	No
FarmIns	Yes	Yes	Yes	Yes	High

faced by insurance providers which could cost a lot. Deployment of IoAT devices can help in monitoring real-time data but lack of device security at IoAT devices also needs to be addressed.

3.2 The Solution Proposed

The proposed solution transitions from centralized to decentralized systems in order to increase transparency and integrity, avoid single points of failure, enhance security and reliability, avoid third parties in an untrusted environment, and secure the automation insurance process. In addition, rather than relying on a single data provider or API service, the farmland is monitored by multiple data providers with value aggregation to ensure accuracy and avoid fake data and single points of failure.

3.3 The Novelty of the Proposed Solution

Proposed FarmIns automates the process of managing crop insurance by leveraging hybrid smart contracts. These hybrid smart contracts consume data from multiple data providers along with weather APIs to provide reliable farm monitoring data to the insurance companies which not only avoids the false claims but also aid in faster processing times. Proposed FarmIns also uses IPFS integrated to blockchain which will reduce the cost of managing large information off-chain instead of expensive on-chain storage. It also makes use of cloud functionalities to act as a Decision Support Tool (DST) for farmers to take prompt actions.

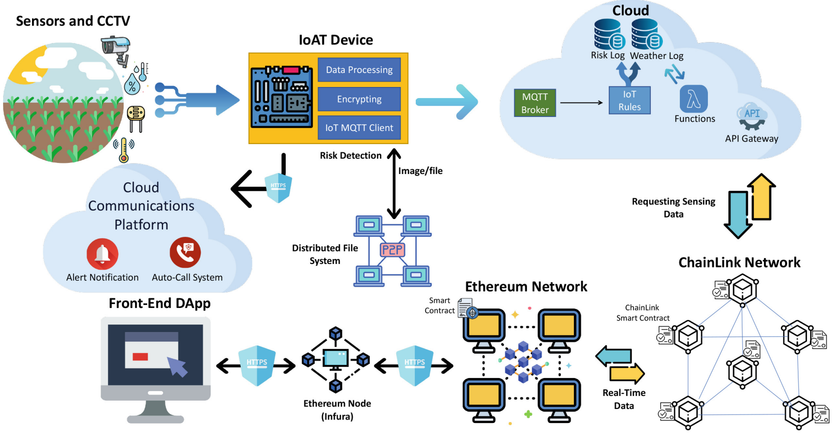


Fig. 1. FarmIns Architecture.

4 FarmIns Architecture

FarmIn's framework is comprised of various technologies that collaborate to provide a reliable and scalable system. IoAT devices are used to sense environmental parameters and create a real-time monitoring system. These steps are shown in Fig. 1. IoAT devices creates a secure channel to cloud using key and certificate authority (CA) files. Data from sensors will be relayed to cloud by using lightweight Message Queuing Telemetry Transport (MQTT) protocol. Sensory data received in cloud is processed based on predefined set of rules to check for abnormalities. These abnormalities will trigger a simple notification for farmers to take prompt actions and mitigate crop losses. In case of abnormal values, IoAT device also takes pictures of surroundings and will be uploaded to the distributed file system Inter Planetary File System (IPFS). Cloud component designed in the proposed architecture also makes the sensory data available to decentralized oracles by using Application Programming Interface (API) gateway. Multiple such data providers will provide data to oracle which will aggregate and provide reliable data to smart contracts to automate the process of managing insurance policies.

4.1 Stakeholders

FarmIns has four primary stakeholders: farmer, approved insurance provider (AIP), government agency like Federal Crop Insurance Corporation (FCIC) and

Algorithm 1. Sensing Environmental Variables and Sending It to Cloud

```
Require: Certificates and keys for IoAT thing, Environmental Parameters.
Ensure: Stored in cloud or Discarded.
Sensing node reads and loads and key pairs and Certificates
Create a secure MQTT communication channel to cloud
while (MQTT.status() == connected) do
    conn ← MQTT.connect(CA$_{cert}$,PrK,PuK)
end while
for Every 30 seconds do
    Environmental Parameters (params) ← sensors.read() and converted to a JSON
    JSONString ← JSON.dumps(params)
    Sensing node creates a message (MSG) with all the metadata like Sensing node
    device ID
    MSG ← JSONSTring.append(headers)
    IoAT device sends the data to the cloud using MQTT connection.
    conn.publish(MSG,TopicName)
end for
Cloud Authenticate the IoAT device with $PKI$ and $CA$
if IoAT Authenticated then
    Store the data to the proper action/log DB and with timestamp
else
    Discard
end if
```

the data provider (DP). Approved insurance provider offers crop protection against serves weather and disaster while FCIC shares the risk estimate with AIP and provide subsidy to a farmer to encourage the farmer to insure the farmland. Data providers are utilized to provide accurate weather data to FCIC and AIP for better risk estimate and aid in processing of claims.

4.2 The Proposed Algorithms for FarmIns

As presented in Algorithm 1, each IoAT device connected with different sensors such as GPS Module, water level detection and temperature sensors. The environmental parameters collected are first converted into JSON format before sending it to the cloud component which acts as data provider for the distributed data source. Each IoAT device has their own keys and certificates to create a secure communication channel to the cloud using lightweight communication protocol.

Algorithm 2 explains the process of getting data from the cloud until stored to the blockchain.

5 Implementation and Validation

5.1 Implementation

FarmIns implementation consists of hardware and software tools. The hardware tools are raspberry Pi 4 Model B as IoAT device and used sensors to measure the environmental variables as presented at Fig. 2. The software parts are solidity programming language to write hybrid smart contracts and react.js and web3.js for building web interface and smart contract interaction as end-user application. Cloud component is designed to act as data provider network for distributed data source Oracle.

Algorithm 2. From Cloud to stored on Blockchain

```
Require: Weather Data and data from sensing node.
Ensure: A transaction hash with an immutable log generated in blockchain ledger.
Insurance provides calls the data smart contract to fetch environmental data
for Each call do
    dataSmartContract.fetchWeatherParams() only InsuranceProvider()
    for Each Data Provider do
        fetchWeatherParams function creates a chainlink request with given Oracle
        Job ID (JID)
        request (req) ← buildChainlinkRequest(JID, msg.sender,fulfill function)
        API url is updated to the request
        req ← req.add(url)
        Path to the data in the response is added to the request
        req ← req.addPath(Path of weather data in JSON response)
        Chainlink request is sent to fetch data
        Obtain the weather data through API gateway
        weatherData ← sendChainlinkRequest(req)
    end for
    Obtained the accurate values through Oracle aggregator contract
    Smart Contract generates an event with the weather data and store the data
end for
```

Table 2. Load Test Results

Test Number	Number of Messages	Elapsed Time (seconds)	Messages per Second
1	400	0.03192	12541.56
2	600	0.04258	14089.87
3	1200	0.09153	13109.55
4	1600	0.18477	8659.97

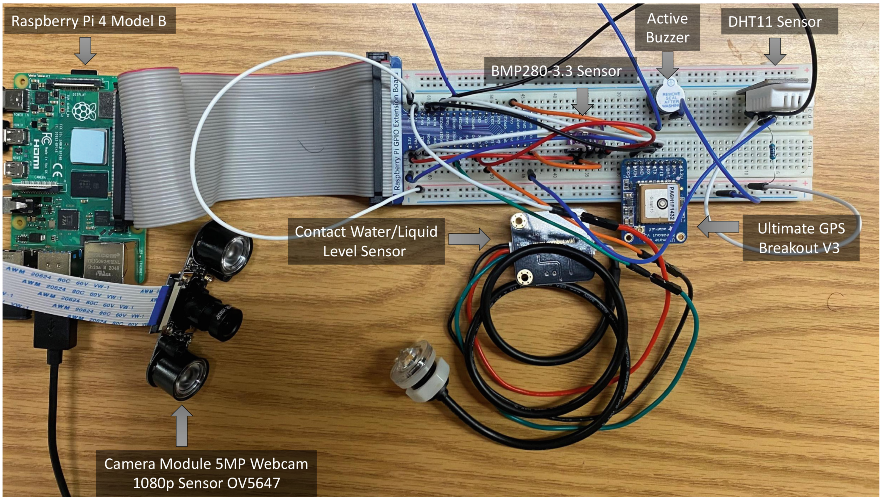


Fig. 2. Hardware Implementation.

5.2 FarmIns Validation

5.3 Cost Analysis and Time Analysis

The cost analysis is divided into two major parts: deployment cost analysis for smart contracts and functional cost analysis. The average cost of smart contract deployment is 0.005787 ETH. While the average functional cost analysis is 0.0007724 ETH, each data fetch from decentralized data source costs 0.1 LINK tokens. All these costs can be avoided by using private networks. Figure 3 presents the time consumed from sensing operation till the environmental data stored on cloud which acts as data provider. Table 2, it demonstrates the system's performance and responsiveness with respect to different loads.

5.4 Security Analysis

The proposed FarmIns architecture ensure data integrity and device authentication for IoAT devices using public key infrastructure (PKI). This prevents the false weather or environmental parameters entered into the system. Role Based Access Control (RBAC) mechanism is implemented in proposed FarmIns to ensure different entities participating in the network will have their own functions which cannot be accessed by other entities with different roles. Transparent and single source of truth ledger is provided by utilizing blockchain which ensures the auditability of the proposed system. Along with all these, implementing oracle which integrates the data from multiple data providers and provide reliable data to the smart contracts ensures the data security.

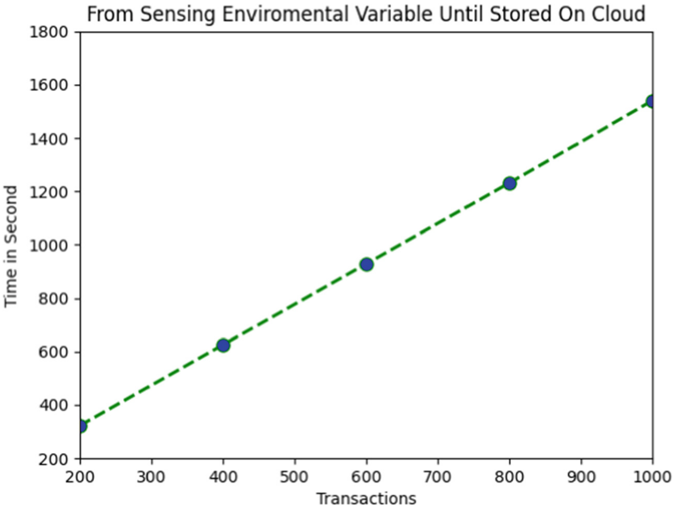


Fig. 3. Time Analysis.

6 Conclusion

Proposed FarmIns system avoids many problems with traditional crop insurance systems such as faster processing of insurance claims by automating the procedures using smart contracts. Blockchain usage provides single source of truth which transparent across all the distributed entities in the system, which increases trust in the network. FarmIns also makes use of environmental parameters of the farm collected using IoAT which will give a better damage estimate in case of claims. Cloud functions are also implemented which act as DST for farmers that assist in taking prompt actions and avoid any extensive crop damages. Implementing hybrid smart contracts combined with Oracle ensure, data fed into the blockchain network is reliable.

References

1. Nguyen, T.Q., Das, A.K., Tran, L.T.: Neo smart contract for drought-based insurance. In: 2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE), pp. 1–4 (2019)
2. Salem, M.J., Ndolu, F.H.E., Hidayatullah, D.E.R., Sari, R.F.: Developing neo smart contract for weather-based insurance. In: 2021 4th International Seminar on Research of Information Technology and Intelligent Systems (ISRITI), pp. 603–608 (2021)
3. Jha, N., Prashar, D., Khalaf, O., Alotaibi, Y., Alsufyani, A., Alghamdi, S.: Blockchain based crop insurance: a decentralized insurance system for modernization of Indian farmers. Sustainability **13**, 08 (2021)
4. Gera, J., Palakayala, A.R., Rejeti, V.K.K., Anusha, T.: Blockchain technology for fraudulent practices in insurance claim process. In: 2020 5th International Conference on Communication and Electronics Systems (ICCES), pp. 1068–1075 (2020)

5. Patel, H., Shrimali, B.: Agrionblock: secured data harvesting for agriculture sector using blockchain technology. ICT Express (2021)
6. Khan, M., Hassan, A., Ali, Md.I.: Secured insurance framework using blockchain and smart contract. Sci. Program. **2021**, 1–11 (2021)
7. Aleksieva, V., Valchanov, H., Huliyan, A.: Implementation of smart contracts based on hyperledger fabric blockchain for the purpose of insurance services. In: 2020 International Conference on Biomedical Innovations and Applications (BIA), pp. 113–116 (2020)

PTSD Detection Using Physiological Markers

Laavanya Rachakonda(✉) and K. C. Bipin

Department of Computer Science, University of North Carolina Wilmington, Wilmington, USA
{rachakondal,bk3723}@uncw.edu

Abstract. This is an extended abstract for a Research Demo Session based on our published work [1]. PTSD has been a major problem in our society and much research has been done along the line to predict and diagnose PTSD. Our method helps to predict PTSD in its early stage with the help of physiological markers which combined with prior information about the patient like PTSD history, exposure to trauma, substance abuse disorder and other information helps to create a risk score with more accuracy. Due to the lack of a public dataset on this domain, we used different uni variate relationships of physiological markers with PTSD to create a multi-modal model using a slight modification of the naive Bayes algorithm. Implementation of a micro-controller along with the cloud IoT platform and a mobile app is created to demo the possibility of the system which helps healthcare providers and users to timely track and monitor PTSD risks with background information and priors accurately.

Keywords: Internet of Things (IoT) · Smart Healthcare · PTSD Detection · Post-Traumatic Stress Disorder · Probability of PTSD · Naive Bayes · Machine Learning

1 Introduction

Post-Traumatic Stress Disorder (PTSD) is a mental health condition that can develop after experiencing or witnessing a traumatic event, such as combat, sexual assault, or a natural disaster. It can cause symptoms like flashbacks, intrusive thoughts, avoidance behaviors, and difficulty sleeping. Treatment for PTSD often involves therapy and medication. Post-traumatic stress disorder is a leading mental disorder that profoundly affects the general population. With 70% of adults experiencing at least one trauma in their lifetime, 6% or 3 in 50 Americans develop PTSD [4]. 94% of rape victims develop PTSD within the first few weeks after their traumatic experience [5]. 9.2% of adults between 45 and 49 develop PTSD [6]. Each year, 11% to 23% of veterans and 30% or 3 in 10 first responders are diagnosed with PTSD [8,9].

The wearable or automated system will monitor the user's mental health, giving warnings and cues when the user is reaching a dangerous level of stress or trauma [7,11]. It can also alert healthcare professionals or family members of the user if the user requires medical attention. In addition, it can provide relaxation techniques to help the user calm down and provide advice on how to better cope with stress. Furthermore, the wearable or automated system can provide support groups for users to connect with others who are going through similar experiences.

Published by Springer Nature Switzerland AG 2024
D. Puthal et al. (Eds.): IFIPIoT 2023, IFIP AICT 684, pp. 390–395, 2024.
https://doi.org/10.1007/978-3-031-45882-8_27

1.1 Motivation

PTSD has been silently affecting our society in many ways [2]. Treatment and diagnosis have been problematic due to stigma and improper or late diagnosis. We want to build a system that will help with early diagnosis and monitor the patient's health during and after treatment. This will ensure the prevention of complications by notifying the user of the health status early on as well as constant monitoring. We also wanted it to be such that the user's data is never disclosed or used on the server. The data just stays in the system momentarily before it is accessed by the mobile app and because our system will predict the results and run on the mobile app rather than the server it will add that extra layer of security and caution.

2 The Proposed PTSD Prediction System

Using the machine learning algorithm, the obtained physiological data from the user is analyzed. The user will be provided with the probability of development. The device prototype along with the long-term extension of the proposed system is represented in Fig. 1. The data from the wearable will be processed at the edge and will be presented through the mobile application.

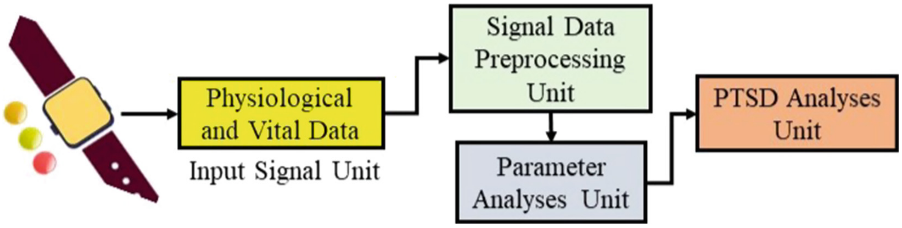


Fig. 1. Proposed Device Prototype of System in the IoT.

2.1 Parameters Considered for the Prediction System

Below are the parameters that are considered for the Machine Learning based PTSD prediction system and the analyses is mentioned in Table 1.

- Heart Rate
- Heart Rate Variability
- Skin Conductance Response
- Blood Pressure
- Respiration Rate

Table 1. Parameter Analyses for PTSD

Heart Rate	Heart Rate Variability	Skin Conductance	Blood Pressure	Respiration Rate	PTSD class
93.98, 21.32	1.46, 0.26	32.1, 14.7	121.3, 13.0	20.24, 5.16	PTSD
79.1, 14.5	1.58, 0.22	16.5,15.0	117.8,12.4	18.58,4.29	No PTSD

[a] M - Median; SD- Standard Deviation

Algorithm 1. Working Principle for early detection of PTSD in Tr-Estimate.

```
Declare and initialize the input variables $HR$ for Heart Rate (HR), $HRV$ for Heart Rate Variability (HRV), $BP$ for blood pressure (BP), $SK$ for Skin Conductance (SC), and $RR$ for Respiration Rate (RR) to zero.
Declare and initialize the output variables $PTSD$ for PTSD class, and $nPTSD$ for no PTSD class to zero.
Declare prior probability $PR$ for the general population to 0.06.
while $HR \neq 0$ do
    Start monitoring and gathering physiological signal data which are $HR$, $HRV$, $BP$,$SK$, and $RR$.
    Declare $Mhr$ and $sdhr$ as median, standard deviation of $HR$, $Mhrv$ and $sdhr$ as median, standard deviation of $HRV$, $Mbp$ and $sdbp$ as median, standard deviation of $BP$, $Msk$ and $sdsk$ as median, standard deviation of $SK$ and $Mrr$ and $sdrr$ as median, standard deviation of $RR$.
    Initialize the above-declared variables to the data from Table 1.
    Posterior probability is calculated and is assigned to $pr$ for each class. These are P($HR|PTSD$), P($HRV|PTSD$), P($RR|PTSD$), P($HR|nPTSD$), P($RR|nPTSD$) and so on.
    Using prior priorities $PP$ for each subclass from above.
    Using $PP$ and $pr$, score for $PTSD$ class $sc_PTSD$ and for $nPTSD$ class $sc_nPTSD$ are calculated.
    Relative score or the ratio is calculated by dividing $sc_PTSD$ and $sc_nPTSD$
end while
```

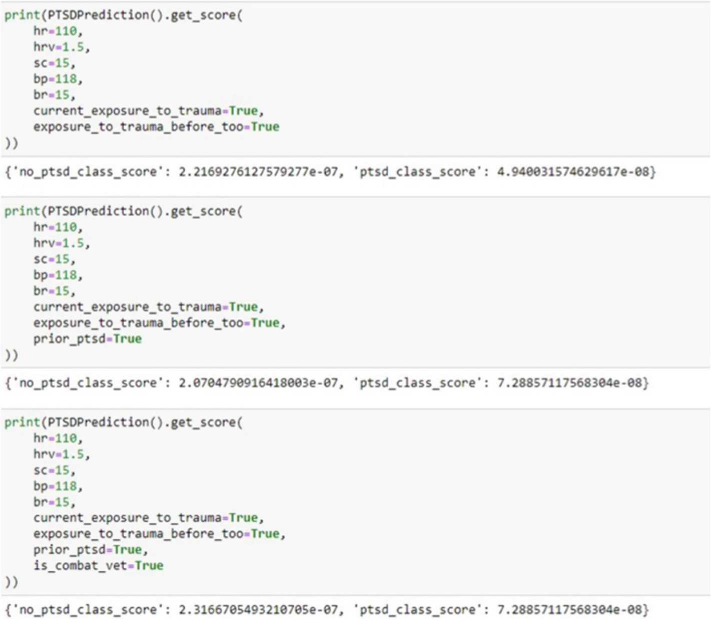
2.2 Working of the Proposed Prediction System

Below is the algorithm for the proposed PTSD prediction system 1.

3 Implementation

The probability classification for the two levels - PTSD and no PTSD are again subcategorized into:

- **Subclass 1**: Adults who have recently been exposed to traumatic incidents (less than three months). The prior probability for these adults is 0.18 [10].
- **Subclass 2**: Adults who have been exposed to previous trauma (more than three months) along with the recent exposure to trauma. The prior probability of these adults is 0.122 [10].
- **Subclass 3**: Adults who were exposed to current and past trauma and were diagnosed with prior PTSD have a prior probability of 0.083 [10].

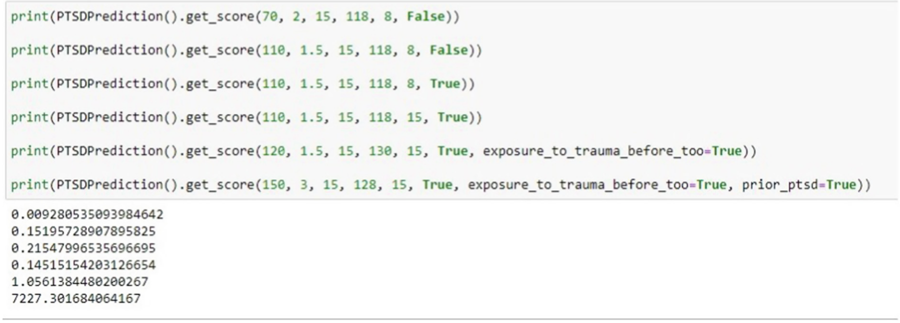


```
print(PTSDPrediction().get_score(
    hr=110,
    hrv=1.5,
    sc=15,
    bp=118,
    br=15,
    current_exposure_to_trauma=True,
    exposure_to_trauma_before_too=True
))
{'no_ptsd_class_score': 2.2169276127579277e-07, 'ptsd_class_score': 4.940031574629617e-08}

print(PTSDPrediction().get_score(
    hr=110,
    hrv=1.5,
    sc=15,
    bp=118,
    br=15,
    current_exposure_to_trauma=True,
    exposure_to_trauma_before_too=True,
    prior_ptsd=True
))
{'no_ptsd_class_score': 2.0704790916418003e-07, 'ptsd_class_score': 7.28857117568304e-08}

print(PTSDPrediction().get_score(
    hr=110,
    hrv=1.5,
    sc=15,
    bp=118,
    br=15,
    current_exposure_to_trauma=True,
    exposure_to_trauma_before_too=True,
    prior_ptsd=True,
    is_combat_vet=True
))
{'no_ptsd_class_score': 2.3166705493210705e-07, 'ptsd_class_score': 7.28857117568304e-08}
```

Fig. 2. Example Scores that were Generated.



```
print(PTSDPrediction().get_score(70, 2, 15, 118, 8, False))

print(PTSDPrediction().get_score(110, 1.5, 15, 118, 8, False))

print(PTSDPrediction().get_score(110, 1.5, 15, 118, 8, True))

print(PTSDPrediction().get_score(110, 1.5, 15, 118, 15, True))

print(PTSDPrediction().get_score(120, 1.5, 15, 130, 15, True, exposure_to_trauma_before_too=True))

print(PTSDPrediction().get_score(150, 3, 15, 128, 15, True, exposure_to_trauma_before_too=True, prior_ptsd=True))
0.009280535093984642
0.15195728907895825
0.21547996535696695
0.14515154203126654
1.0561384480200267
7227.301684064167
```

Fig. 3. Scores for Classes - PTSD and No PTSD.

The probability scores are mentioned in Fig. 2.

The scores with various parameters is represented in Fig. 3.

An example of heat map of subclass 3, adults who have been exposed to previous and current trauma and have been diagnosed with PTSD in the past is represented in Fig. 4 by varying blood pressure and skin conductance.

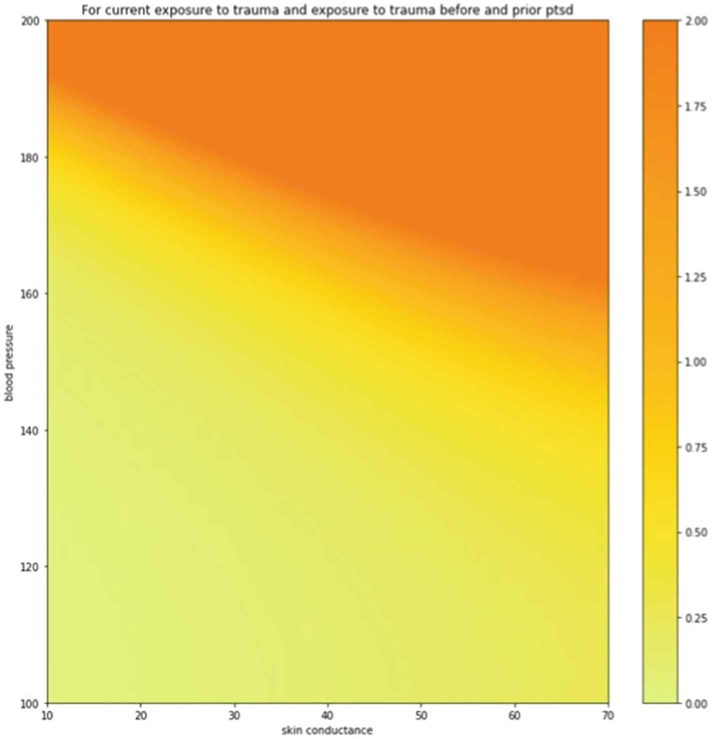


Fig. 4. Heat map for Subclass 3.

4 Conclusions and Future Work

With the analysis and modification of the Bayes rule, we found that even with independent analysis of variables we can get satisfactory results from the naïve Bayes algorithm, and with this method, we can include many independent analyses and combine them to give a meaningful single result. The use of preexisting priors for many subgroups as done in the implementation gives more accurate information and shows how risk scores vary even with the same physiological markers across the groups. This helps in identifying patients' status more accurately and thus leads to a complete and holistic understanding of the patient's risk. Alongside, with the implementation done using IoT and mobile applications, it is shown that such sensitive health concerns can be tracked and used as a supervision tool, diagnostic helper, and early warning tool for people, especially for people who have been recently exposed to trauma and veterans.

With the results obtained about the relationship of different physiological markers, we can see and visualize how these markers interact. We are also able to see how the base score that we got just from the markers is bumped higher or lower based on the different subgroups the users fall under.

For the future development, a robust model will be designed which will be an enhanced version of the current classifier model. The surrounding data will be analyzed and recorded at the occurrence of every event. Along with the prediction of PTSD, control remedies will also be provided to the users to control the transition to the diagnosis of PTSD. Adapting virtual reality technology as a control remedy will also be considered. Creating more robust smart healthcare models to monitor, analyze and educate the users is the main research focus.

References

1. Rachakonda, L., Bipin, K.C.: Tr-Estimate: A Novel Machine Learning Based Early Prediction System for Post-Traumatic Stress Disorder using IoMT. In: 2022 IEEE International Symposium on Smart Electronic Systems (iSES), pp. 677–682. Warangal, India (2022). https://doi.org/10.1109/iSES54909.2022.00151
2. Rachakonda, L., Mohanty, S.P., Kougianos, E., Sundaravadivel, P.: Stress-Lysis: a DNN-integrated edge device for stress level detection in the IoMT. IEEE Trans. Consum. Electron. (TCE) **65**(4), 474–483 (2019)
3. Rachakonda, L., Mohanty, S.P., Kougianos, E.: iLog: an intelligent device for automatic food intake monitoring and stress detection in the IoMT. IEEE Trans. Consum. Electron. (TCE) **66**(2), 115–124 (2020)
4. PTSD: National Center for PTSD: How Common Is PTSD in Adults?, U.S. Department of Veterans Affairs. https://www.ptsd.va.gov/understand/common/. Accessed Aug (2022)
5. Rothbaum, B., Foa, E., Riggs, D., Murdock, T., Walsh, W.: A prospective examination of post-traumatic stress disorder in rape victims. J. Traumatic Stress **5**(3), 455–475 (1992)
6. Kessler, R.C., Berglund, P., Demler, O., Jin, R., Merikangas, K.R., Walters, E.E.: Lifetime Prevalence and Age-of-Onset Distributions of DSM-IV Disorders in the National Comorbidity Survey Replication. Arch. General Psych. **62**(6), 593–602 (2005)
7. Rachakonda, L., Bapatla, A.K., Mohanty, S.P., Kougianos, E.: SaYoPillow: blockchain-integrated privacy-assured IoMT framework for stress management considering sleeping habits. IEEE Trans. Consum. Electron. (TCE) **67**(1), 20–29 (2021)
8. Berghammer, L., Marx, M.F., Odom, E., Chisolm, N.: Wounded Warrior Project. Annual Warrior Survey. Longitudinal: Wave 1, Tech. Rep. (2022). https://www.woundedwarriorproject.org/media/4ptekte3/2021-report-of-findings.pdf
9. SAMHSA: First Responders: Behavioral Health Concerns, Emergency Response, and Trauma, https://www.chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/, https://www.samhsa.gov/sites/default/files/dtac/supplementalresearchbulletin-firstresponders-may2018.pdf
10. Breslau, N., Peterson, E.L., Schultz, L.R.: A second look at prior trauma and the post-traumatic stress disorder effects of subsequent trauma: a prospective epidemiological study. Arch. General Psych. **65**(4), 431–437 (2008)
11. Rachakonda, L., Bapatla, A.K., Mohanty, S.P., Kougianos, E.: BACTmobile: a smart blood alcohol concentration tracking mechanism for smart vehicles in healthcare CPS framework. Springer Nature Computer Science (SN-CS). **3**(3), 236 (2022). https://doi.org/10.1007/s42979-022-01142-9

A Signal Conditioning Circuit with Integrated Bandgap Reference for Glucose Concentration Measurement

Riyaz Ahmad(✉), Amit Mahesh Joshi, and Dharmendar Boolchandani

Department of Electronics and Communication Engineering, Malaviya National Institute of Technology, Jaipur, Rajasthan 302017, India
2018rec9120@mnit.ac.in

Abstract. The paper presents development of signal conditioning circuit with integrated potentiostat for glucose measurement. The programmable transimpedance amplifier (PTIA) offers 94% linearity of output voltage. The whole architecture consumes 2.33 mW of total power. The reference potential of 0.6 V has been used for measurements. Three electrode arrangement with Ag/AgCl as reference electrode, the Pt foil as the counter electrode and a CuO/$Cu_{0.76}CO_{2.25}O_4$ (copper cobaltite) coated glassy carbon electrode (GCE) filled-in used as the working electrode. The working feasibility of proposed glucose sensing architecture is tested via an emulated circuit. The second-generation current conveyor (CCII-) is implemented with the help of two AD844 ICs. The two TAs are implemented by using IC LM13700 and I-V conversion is obtained with op-amp IC LM741 and feedback resistance. The voltage ranges from 1.19 to 1.67 V has been measured corresponding to glucose concentration ranges from 18 mg/dl to 180 mg/dl.

Keywords: Glucose sensing · Potentiostat · Programmable transimpedance amplifier · Emulated circuit

1 Introduction

One of the fastest-growing health problems, diabetes is brought on by an unbalanced glycemic profile and has tripled in prevalence over the past two decades [1]. The body needs glucose to carry out daily tasks, however the usual range of glucose can be considered from 80 mg/dl to 150 mg/dl [2], hence, must be regularly monitored. An electronic interface architecture based on reference potentiostats and readout circuits is helpful for processing the signals from electrochemical glucose sensors. The literature [3, 4] reviews the interface designs for electrochemical sensing and systems for monitoring level of glucose. In [5], a current-conveyor (CC) based TIA with poor sensitivity for glucose sensing was reported. Digitally adjustable with a complex digital circuit and covering a wide range of sensor current, TIA is proposed in [6]. The readout circuit in [7] measures low range of current within ± 2 μA. In order to detect small sensor currents, Karandikar et al. [8] presented a small design that makes use of a high load resistance. A small range of glucose concentration with a higher power dissipation was discussed in [9, 10].

Published by Springer Nature Switzerland AG 2024
D. Puthal et al. (Eds.): IFIPIoT 2023, IFIP AICT 684, pp. 396–401, 2024.
https://doi.org/10.1007/978-3-031-45882-8_28

A novel contribution of this work are as follows:

- A bandgap reference voltage potentiostat and a programmable readout circuit are combined into a single circuit.
- A block level architecture for glucose sensing has been proposed and its emulated circuit has been developed to demonstrate the working feasibility.

2 Proposed Electronic Interface Architecture for Glucose Sensing Applications

The Fig. 1 depicts a bandgap reference voltage potentiostat and a programmable readout circuits which are used to interface with electrochemical glucose sensor in the proposed electronics architecture block for glucose level measurement. The bandgap reference voltage potentiostat has been designed to produce 0.6 V constant voltage. To establish reference voltage independent of power supply variations, it functions on the theory of levelling parameters with opposing temperature coefficients. As a result, the circuit is independent of supply voltage. In order to prevent the degenerate bias point or zero bias current when the supply voltage is turned on, this bandgap reference circuit needs a start-up circuit. The WE and RE electrodes of an electrochemical sensor are connected to a reference potentiostat.

The sensor current is fed into differential CC to effectively buffer the sensor current. The CC output current is amplified by the PTBTA circuit. The current amplification is done at various levels with the help of control signals given to the PTBTA circuit. Ultimately, the amplified current signal is changed to voltage via current to voltage (I-V) converter and TA circuit feedback arrangement. The detailed CMOS circuit implementation and explanation including noise analysis is available in its longer version literature in [11].

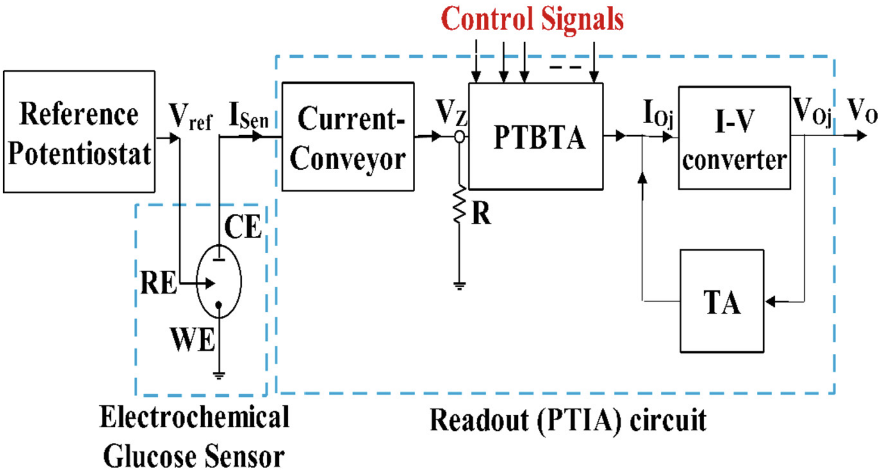


Fig. 1. Block architecture for glucose level monitoring.

3 Electrochemical Measurement: Experimental Setup for Glucose Concentration Measurement

Three-electrode design arrangement with Ag/AgCl as reference electrode and the Pt foil (1 × 2 cm) as the counter electrode. For entire electrochemical experiments, O_2 soaked 0.15 M aqueous NaOH solution was used as electrolyte. The electrocatalyst or working electrode was prepared by ultrasonic dissemination of 1.5 mg of the $CuO/Cu_{0.76}CO_{2.25}O_4$ material to make a homogeneous solution of 550 μL of deionized water and 50 μL of nafion solution (5 wt % in ethanol). The 15 μL of this homogeneous solution was consistently drop projected on a clean GCE (5 mm diameter) trailed by room temperature drying. The precise electrochemical estimations for glucose measurement were executed by cyclic voltammetry (CV) at a specific scan rate of 10 mVs^{-1}, amperometric current versus time measurements at 0.6 V versus Ag/AgCl. The complete setup was emulated for glucose measurement in Fig. 2. The second-generation current conveyor (CCII-) is implemented with the help of two AD844 ICs. The two TAs are implemented by using IC LM13700 and I-V conversion is obtained with op-amp IC LM741 and feedback resistance. The reference voltage of 0.6 V is considered. The measurement setup proves the working feasibility and strengthens the proposed block architecture for glucose sensing. The glucose has been added in four arms beaker in steps of 18 mg/dl after a fixed time interval and upto 180 mg/dl, the measurement has been done. The voltage ranges from 1.19 to 1.67 V has been measured corresponding to glucose concentration ranges from 18 mg/dl to 180 mg/dl as shown in Table 1. The linearity performance of prototyped circuit is shown in Fig. 3.

Table 1. Measured output voltage and glucose concentration relation by experimental setup for glucose sensing.

Sr. Number	Glucose Concentration (mg/dl)	Output Voltage (Volts)
1	18	1.19
2	36	1.31
3	54	1.39
4	72	1.46
5	90	1.52
6	108	1.57
7	126	1.61
8	144	1.64
9	162	1.65
10	180	1.67

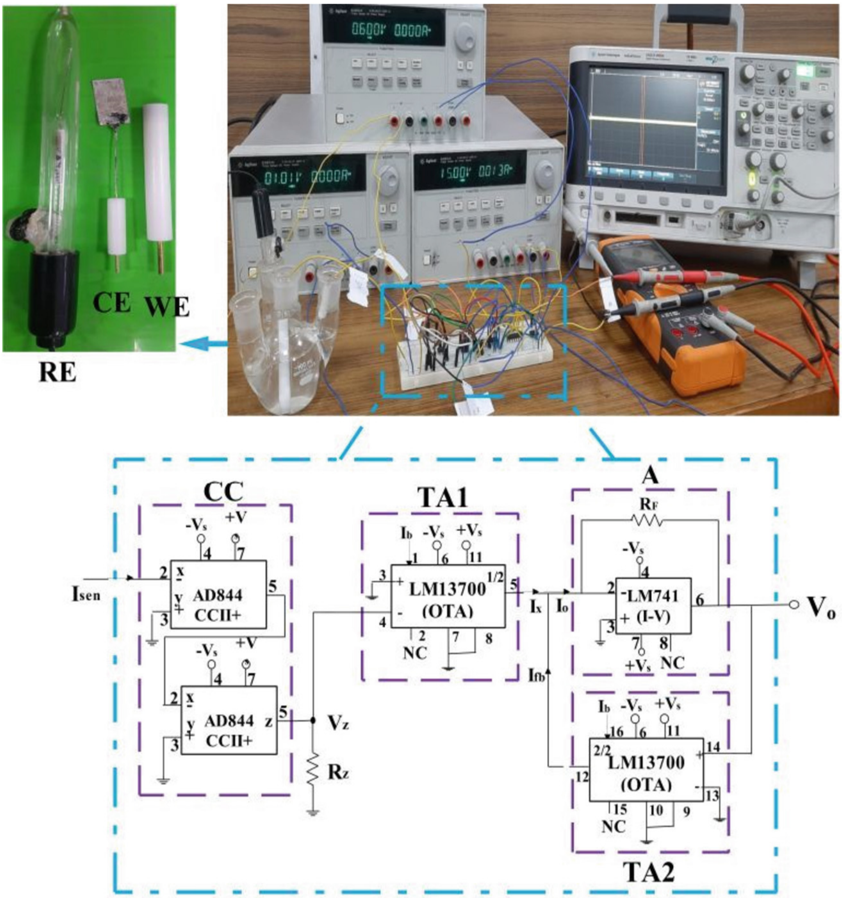


Fig. 2. Experimental setup for glucose concentration measurement with emulated readout circuit.

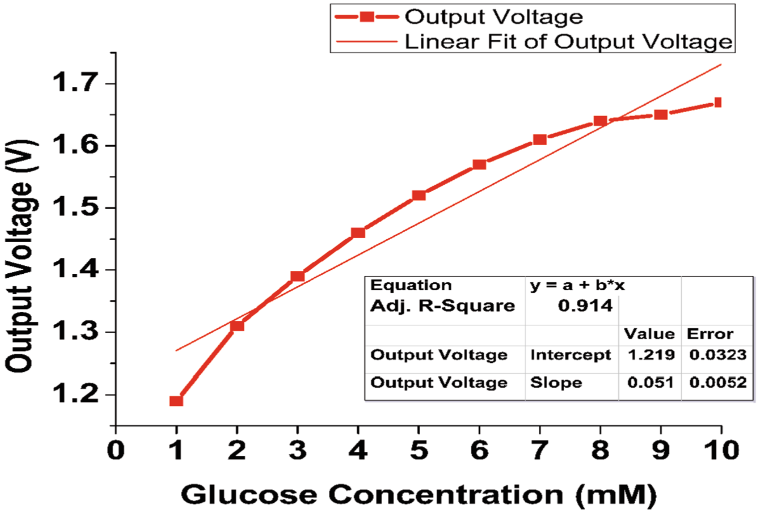


Fig. 3. Measured output voltage and glucose concentration relation and linearity performance.

4 Conclusion

This paper presents a novel electronics interface architecture for glucose sensing applications and measured results by emulated circuit are presented in this paper. The measurement setup is able to detect glucose concentration ranges from 18 mg/dl to 180 mg/dl. The proposed glucose interface architecture produces a linear range of output voltage from 1.19 V to 1.67 V for glucose concentration ranges from 18 mg/dl to 180 mg/dl. The proposed design can also be helpful for detection of other target objects like uric acid, tear and so on used in electrochemical sensing applications.

Acknowledgment. The authors are grateful to VLSI Lab, ECE department MNIT, Jaipur and Materials Electrochemistry and Energy Storage Lab, Chemistry department, MNIT Jaipur for providing the support of EDA tools and measurement setup to conduct the experiments.

References

1. Ahmad, R., Joshi, A.M., Boolchandani, D., Varma, T.: Design of potentiostat and current mode read-out amplifier for glucose sensing. In: 2021 IEEE International Symposium on Smart Electronic Systems (iSES)(Formerly iNiS), pp. 64–69. IEEE (2021)
2. Ahmad, R., Joshi, A.M., Boolchandani, D., Varma, T.: Novel programmable read- out amplifier and potentiostat for glucose sensing applications. SN Computer Science **4**(2), 1–11 (2023)
3. Ying, D., Hall, D.A.: Current sensing front-ends: a review and design guidance. IEEE Sensors Journal (2021)
4. Jain, P., Joshi, A.M., Mohanty, S.P.: iglu 1.1: Towards a glucose-insulin model based closed loop iomt framework for automatic insulin control of diabetic patients. In: 2020 IEEE 6th World Forum on Internet of Things (WF-IoT), pp. 1–6. IEEE (2020)

5. Esparza-Alfaro, F., Pennisi, S., Palumbo, G., Lopez-Martin, A.J.: Lowpower class- ab cmos voltage feedback current operational amplifier with tunable gain and bandwidth. IEEE Trans. Circuits Syst. II Express Briefs **61**(8), 574–578 (2014)
6. Park, H., Lakshminarayana, S., Pan, C., Chung, H.J., Jung, S.: An auto adjustable transimpedance readout system for wearable healthcare devices. Electronics **11**(8), 1181 (2022)
7. Li, M., Vanhoestenberghe, A., Ghoreishizadeh, S.S.: An integrated circuit to enable electrodeposition and amperometric readout of sensing electrodes. In: 2022 IEEE 13th Latin America Symposium on Circuits and System (LASCAS), pp. 1–4. IEEE (2022)
8. Karandikar, N., Jung, S., Sun, Y., Chung, H.J.: Low power, low noise, compact am- perometric circuit for three-terminal glucose biosensor. Analog Integr. Circ. Sig. Process **89**(2), 417–424 (2016)
9. Shenoy, V., Jung, S., Yoon, Y., Park, Y., Kim, H., Chung, H.J.: A cmos analog correlator-based painless nonenzymatic glucose sensor readout circuit. IEEE Sens. J. **14**(5), 1591–1599 (2014)
10. Ghoreishizadeh, S.S., Taurino, I., De Micheli, G., Carrara, S., Georgiou, P.: A differential electrochemical readout asic with heterogeneous integration of bio-nano sensors for amperometric sensing. IEEE Trans. Biomed. Circuits Syst. **11**(5), 1148–1159 (2017)
11. Ahmad, R., Joshi, A.M., Boolchandani. D.: Programmable Transimpedance Amplifier with Integrated Bandgap Reference for Glucose Concentration Measurement. arXiv preprint arXiv:2305.12503 (2023)

Detection of Aircraft in Satellite Images using Multilayer Convolution Neural Network

Swaraj Agarwal[1], Narayan Panigarhi[2](✉), and M. A. Rajesh[2]

[1] Gautam Buddha University, Greater Noida, U.P., India
[2] Centre for Artificial Intelligence and Robotics, Bangalore, Karnataka, India
npanigrahi7@gmail.com

Abstract. The automatic identification of various spatial entities within satellite imagery is a crucial undertaking for interpreting such images. Numerous research papers have explored the segregation, identification, and geolocation of objects of interest, such as airplanes, vehicles, and human elements, within satellite images. The detection of aircraft from satellite imagery is particularly significant for gathering operational intelligence. Detecting aircraft within the environment is achieved through active remote sensing methods, such as RADAR and LASER. Various algorithms have been devised and developed specifically for aircraft detection in satellite imagery. The advent of AI-based techniques has brought about a transformative shift in object detection within remotely sensed images. This paper proposes a methodology employing a convolutional neural network (CNN) for the detection of aircraft within satellite imagery. Initially, an image dataset is generated using QGIS software, which is then partitioned into training and testing datasets. A multi-layered CNN model is employed to train and evaluate the dataset. Subsequently, the trained CNN is applied to remotely sensed images to detect the presence of aircraft within the scene. The aircraft detection accuracy from randomly selected satellite images is reported to be 95%.

1 Introduction

The identification of objects of significance within satellite imagery has emerged as a crucial research area in remote sensing. Traditional approaches rely on human interpreters with specialized training to detect these objects. However, the increasing influx of high-frequency satellite images has rendered this manual detection process cumbersome and inefficient. As a result, several algorithms have been proposed to automate the detection of objects of interest in these images. In recent times [5–9], there has been a surge in research focused on AI-based algorithms for object detection in remote sensing images. In this paper, we present a CNN-based method for the detection of aircraft in satellite images. The implementation and testing of our CNN model have demonstrated superior performance compared to computationally driven object detection algorithms.

Artificial intelligence offers a significant advantage in the field of Geographic Information Systems (GIS) [13] by enabling comprehensive analysis of various aspects using image data. These images can be obtained either from satellites or aerial vehicles. The

Published by Springer Nature Switzerland AG 2024
D. Puthal et al. (Eds.): IFIPIoT 2023, IFIP AICT 684, pp. 402–409, 2024.
https://doi.org/10.1007/978-3-031-45882-8_29

analysis can encompass a wide range of applications, including environmental impact analysis, accident analysis, hotspot analysis, telecom and network systems, mapping and surveying, agricultural applications, navigation, natural resource management, irrigation and water management, and defense, with a specific focus on the defense domain.

Various systems, such as RADAR and aerial vehicles, have been widely utilized for object detection and identification. However, these systems are limited in their range and can typically detect objects within a few hundred kilometers. To gather information about a distant plot of land, satellite images are the primary source. Previously, object detection in images relied on algorithms such as Support Vector Machine (SVM), Histogram of Oriented Gradient (HOG), and Scale Invariant Feature Transformation (SIFT). However, these algorithms were characterized by slow processing speeds and relatively lower accuracy. The advent of multi-layer convolutional neural network (CNN) models has revolutionized object detection in images, enabling highly accurate identification of objects with improved efficiency.

2 Related work

Extensive research has been conducted on the topic of aircraft detection in satellite images, with each method presenting its own strengths and weaknesses. The following research studies highlight some notable findings:

In this study [1, 10, 12], a CNN model is employed to generate edge boxes on high-resolution satellite images. The analysis focuses on aircraft and oil tank datasets, utilizing R-CNN, edge boxes, DBN, and HOG SVM models. The recall rate achieved for aircraft detection using R-CNN is 81.66%, while edge boxes DBN achieves a rate of 77.70%. For oil tank detection, the recall rate using R-CNN is 46.56%, whereas edge boxes DBN achieves 86.88%. However, the R-CNN model struggles with detecting small objects, resulting in lower accuracy for oil tank detection. Additionally, this model only provides bounding boxes without labelling the contents, and training is limited to passenger aircraft.

In this research [2], aircraft detection is performed using LOCNet-C, SPMK, and UFL methods. The findings indicate that LOCNet-C outperforms the other methods in terms of accuracy. However, while the location of the aircraft is detected, the specific identification of aircraft types is not provided.

This study [3] focuses on aircraft detection using Faster R-CNN on a dataset comprising 265 images from various airports. The dataset is divided into training and testing sets, with 10% used for testing. The achieved accuracy is reported to be 53.64%. However, single object detection is not addressed in this research.

In this research [4, 11], CNN and R-CNN methods are employed, where CNN is used to detect aircraft and R-CNN is utilized to generate regions. The detection is binary, indicating the presence or absence of an aircraft. The achieved accuracy for this approach is reported to be 98.40%.

3 The Experimental Work

Satellite images play a crucial role in safeguarding national security interests, allowing for surveillance of enemy countries. In this study, extensive exploration within the GIS domain aims to identify military aircraft in satellite images, particularly during warfare or other security operations. To achieve this, a multi-layered convolutional neural network (CNN) model is employed for the detection of both military and civilian aircraft. The dataset used in this research has been gathered through the utilization of QGIS software, an open-source tool widely used for geospatial analysis and mapping.

The test dataset was generated using the following procedure. First, the QGIS software was installed, followed by the installation of the ‘quickmapservices’ repository, which allows loading the base map into the QGIS project. Then, in the toolbar, the ‘web’ option was selected, followed by ‘quickmap’. This displayed a list of satellite images captured by various sensors. An image from any desired company was selected. The airport’s location was then browsed, and the ‘new print layout’ option was chosen, opening a dialogue box. In the dialogue box, ‘add maps’ was clicked, and the area of interest within the image was selected. The image was saved with the desired pixel size.

The dataset was created using various aircraft images of different shapes and sizes. Subsequently, the dataset was divided into training and testing sets. The multi-layer CNN model was then applied to this dataset. The images in the dataset could be either black and white or color images with an RGB palette. In a computer system, each image is represented as a matrix of intensity values, with values ranging from 0 to 225.

The steps to build the CNN model are

a. **Convolution:** Convolution is a fundamental operation in image processing and serves as a feature extraction method. It involves extracting features from an image by applying a kernel or filter through a dot product operation. This process allows the CNN to detect patterns, edges, textures, and other visual features within the image data. The convolution operation plays a crucial role in enabling the network to learn and understand the underlying characteristics of the images it analyzes.

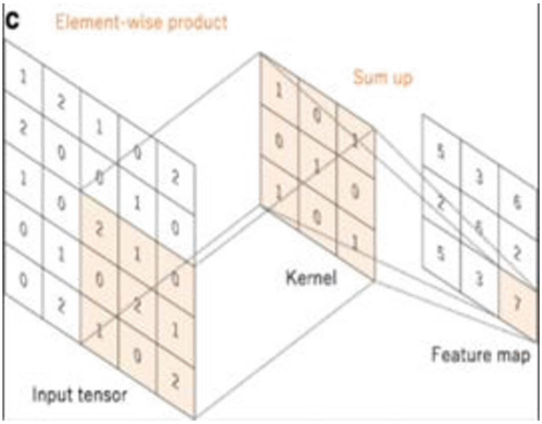


Fig. 1. Represents the convolution process

In a CNN model, the input tensor represents the input image in an array format. The kernel, also known as a filter or a convolutional filter, is a mathematical matrix that enables the application of a linear classifier to a non-linear problem. The convolution operation involves performing a dot product between the kernel and each element of the input image. This process includes element-wise multiplication of corresponding elements followed by summation of the results. The resulting value is then placed in the corresponding location of the feature map. This operation helps extract and identify important features in the image, as illustrated in Fig. 1.

$$(1*1)+(2*0)+(1*1)+(2*0)+(1*0)+(0*0)+(1*1)+(0*0)+(1*2)$$
$$=1+0+1+0+0+0+1+0+2=5$$

Pooling:

Pooling layers are indeed utilized in CNN models to reduce the dimensionality of the feature map. There are various types of pooling, including Max pooling, Mean pooling, and Min pooling. In this case, max pooling is being employed as it has been observed to provide better accuracy compared to other pooling techniques. During max pooling, the maximum value within the specified pooling region is selected and used as the output. In the provided example, a 2x2 pooling kernel is used. As illustrated, the maximum value in the first pooling region is 8, so that value is chosen as the output (Fig. 2).

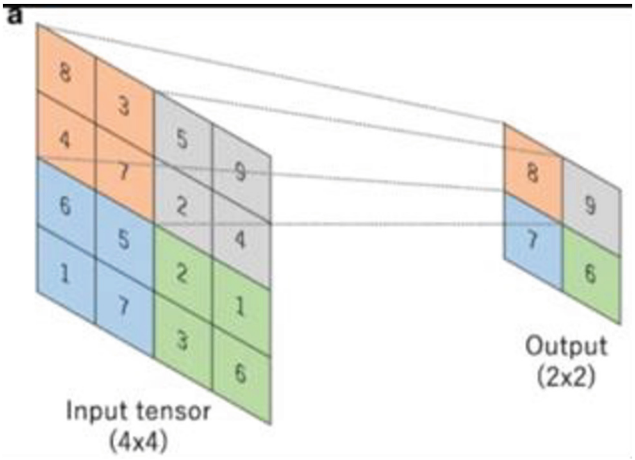


Fig. 2. Represents the max pooling to an input tensor

c. **Flattening layer:**

Flattening layers play a crucial role in a CNN model by taking the outputs of the preceding pooling layers and arranging them into arrays or vectors. These flattened arrays are then passed as input to the subsequent layers in the network. In Fig. 3, which represents the flattening layer, the outputs from the pooling layer are reshaped into a one-dimensional array, allowing for seamless connectivity with the following layers in the network. This transformation enables the network to efficiently process and learn from the extracted features in preparation for further analysis or classification tasks.

d. **Fully connected layer:**
In a fully connected layer of a neural network, each neuron is connected to every neuron in the previous layer. The number of neurons in the fully connected layer needs to be determined to achieve better accuracy based on the specific task at hand. In the context of CNNs, the flattened array from the preceding layers serves as the input to the fully connected layer.

If the desired output is binary (e.g., for binary classification tasks), the sigmoid function is commonly used as the activation function in the fully connected layer. The sigmoid function maps the output of each neuron to a value between 0 and 1, providing a probability-like interpretation for binary classification.

If the output has more than two classes (multiclass classification), the SoftMax function is typically used as the activation function in the fully connected layer. The SoftMax function assigns probabilities to each class, ensuring that the sum of the probabilities for all classes adds up to 1. This allows for the prediction of the most likely class among the available options.

The choice of activation function in the fully connected layer depends on the nature of the problem being addressed and the desired output format.

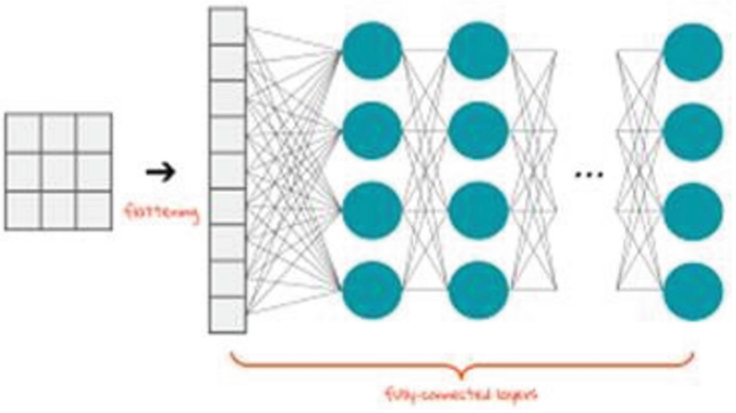


Fig. 3. Represents the fully connected layer

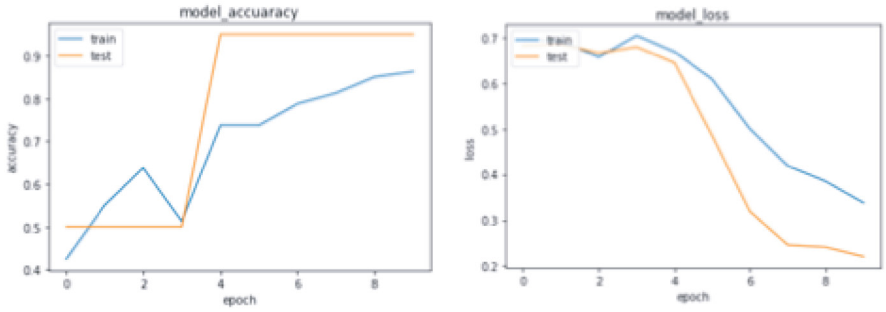
4 Result and Discussion

The implementation of a multilayer CNN has been successfully employed as a supervised method to detect both civilian and military aircraft. The CNN model consists of 11 layers, including 4 convolutional layers with varying input shapes (150, 150, 3), 4 max pooling layers, 1 flattening layer, and 2 fully connected layers for weight assignment and prediction.

In the experiment, a dataset was created using the QGIS software. The training dataset comprised 50 images of civilian aircraft and 50 images of defence aircraft. The dataset was then split into training and testing sets, with 80% of the data used for training and 20% for testing. The training was performed with 10 epochs, and an accuracy of 95% was achieved in identifying aircraft objects.

To assess the effectiveness of the training, testing was conducted using the remaining images, which included a random mixture of civilian and defence aircraft. The prediction outputs accurately predicted and identified the aircraft, as shown in Fig. 4-A. The model achieved an accuracy of 95% for both the training and testing sets. The training curve, represented by the blue line, shows a lower accuracy compared to the test curve, represented by the orange line, as observed from the graph.

In Fig. 4-B, the model loss is depicted by the blue curve, which represents the training set, while the orange line represents the test set. It is observed that when there were 20 images used for testing purposes, there was a sudden increase in loss between the 2nd and 4th epoch values. However, as the training progressed, the loss gradually decreased and eventually recovered after reaching the 10th epoch value. This indicates that the model was able to learn and adjust its weights to better fit the training data, resulting in a reduced loss and improved performance on the test set.



A)

B)

Fig. 4. Represents the result of the accuracy and loss model

5 Conclusion

The integration of AI in the GIS defence domain has proved to be highly beneficial, particularly in the field of image processing. In the specific context of aircraft detection, the application of CNN to the created dataset has yielded successful results. By employing a supervised learning approach with an 11-layer CNN model, the dataset was effectively filtered and trained.

The CNN model has demonstrated its capability to accurately detect and classify both civilian and military aircraft, achieving an impressive accuracy rate of 95%. This indicates the effectiveness of the trained model in accurately identifying and distinguishing between different types of aircraft.

By leveraging the power of AI and CNN algorithms, the defence sector can benefit from improved capabilities in aircraft detection and monitoring, leading to enhanced situational awareness and security measures. The high accuracy achieved in this study highlights the potential of AI-based solutions in the GIS defence domain.

The need to accurately locate multiple objects within a single image has led to advancements beyond the capabilities of Convolutional Neural Networks (CNNs). While CNNs are effective in object detection, they do not inherently provide the precise location of objects within the image. This limitation opens opportunities for further development and the future scope of research.

To address this, a method called Faster R-CNN (Region-based Convolutional Neural Network) has been introduced. Faster R-CNN enables the identification of the exact location of specific objects within an image by creating bounding boxes around each object of interest.

Faster R-CNN combines the power of CNNs with a region proposal network (RPN) to generate accurate object proposals. The RPN identifies potential object regions within the image, and then the CNN is employed to classify and refine these proposals, ultimately determining the exact location of the objects.

By integrating Faster R-CNN into the object detection pipeline, researchers and practitioners can achieve both accurate object detection and precise localization, resulting in more comprehensive and detailed analysis of images. This approach has immense potential for various applications, including object recognition, tracking, and scene understanding, contributing to advancements in the field of computer vision and image processing.

References

1. Wu, H., Zhang, H., Zhang, J., Xu, F.: Typical target detection in satellite images based on convolutional neural networks. In: 2015 IEEE International Conference on Systems, Man, and Cybernetics, pp. 2956–2961 (2015). https://doi.org/10.1109/SMC.2015.514
2. Zhang, F., Du, B., Zhang, L., Xu, M.: Weakly supervised learning based on coupled convolutional neural networks for aircraft detection. IEEE Trans. Geosci. Remote Sens.Geosci. Remote Sens. **54**(9), 5553–5563 (2016). https://doi.org/10.1109/TGRS.2016.2569141
3. Wu, H.,Zhang, H., Zhang, J., Xu, F.: Fast aircraft detection in satellite images based on convolutional neural networks. In: 2015 IEEE International Conference on Image Processing (ICIP), pp. 4210-4214 (2015). https://doi.org/10.1109/ICIP.2015.7351599
4. Ucar, F., Dandil, B., Ata, F.: Aircraft detection system based on regions with convolutional neural networks. Int. J. Intell. Syst. Appl. Eng. **8**(3), 147–153 (2020)
5. Radovic, M., Adarkwa, O., Wang, Q.: Object recognition in aerial images using convolutional neural networks. J. Imaging. **3**(2), 21 (2017). https://doi.org/10.3390/jimaging3020021
6. Deng, Z., Sun, H., Zhou, S., Zhao, J., Zou, H.: Toward fast and accurate vehicle detection in aerial images using coupled region-based convolutional neural networks. IEEE J. Selected Topics in Applied Earth Observations and Remote Sensing **10**(8), 3652–3664 (2017). https://doi.org/10.1109/JSTARS.2017.2694890
7. Deng, Z., Sun, H., Zhou, S., Zhao, J., Lei, L., Zou, H.: Multi-scale object detection in remote sensing imagery with convolutional neural networks. ISPRS J. Photogrammetry and Remote Sensing **145**(Part A), 3–22 (2018). ISSN 0924–2716

8. Cheng, G., Zhou, P., Han, J.: Learning rotation-invariant convolutional neural networks for object detection in vhr optical remote sensing images. IEEE Trans. Geosci. Remote Sens.Geosci. Remote Sens. **54**(12), 7405–7415 (2016). https://doi.org/10.1109/TGRS.2016.2601622
9. Fu, K., Chang, Z., Zhang, Y., Xu, G., Zhang, K., Sun, X.: Rotation-aware and multi-scale convolutional neural network for object detection in remote sensing images. ISPRS J. Photogrammetry and Remote Sensing **161**, 294–308 (2020). ISSN 0924–2716
10. Guo, W., Yang, W., Zhang, H., Hua, G.: Geospatial object detection in high resolution satellite images based on multi-scale convolutional neural network. Remote Sens. **10**, 131 (2018)
11. Alshaibani, W.T., Helvaci, M., Shayea, I., Mohamad, H.: Airplane Detection Based on Mask Region Convolution Neural Network. arXiv preprint arXiv:2108.12817 (2021)
12. Xu, Y., Zhu, M., Xin, P., Li, S., Qi, M., Ma, S.: Rapid airplane detection in remote sensing images based on multilayer feature fusion in fully convolutional neural networks. Sensors **18**(7), 2335 (2018). https://doi.org/10.3390/s18072335
13. Panigrahi, N.: Geographic Information Science, 4th ed. Universities Press (India) Private Limited, Hyderabad (2008). ISBN (13) 978-1-4398-1004

PEP: Hardware Emulation Platform for Physiological Closed-Loop Control Systems

Shakil Mahmud(✉), Samir Ahmed, and Robert Karam

University of South Florida, Tampa, FL 33620, USA
shakilmahmud@usf.edu

Abstract. Physiological closed-loop control systems (PCLCS) provide reliable and efficient treatment in medical care, but it is crucial to ensure patient safety when examining the potential advantages. Traditional animal and clinical studies are resource-intensive and costly, making them impractical for evaluating PCLCS in every relevant clinical scenario. Therefore, computational or mathematical models have emerged as an alternative for assessing PCLCS. Hardware-in-the-loop testing platforms can provide a more efficient alternative to traditional animal and clinical studies. The platforms utilize computational or mathematical models to simulate PCLCS, providing a cost-effective and efficient approach that can minimize errors during the development process. Although various software simulation platforms can model specific physiological systems, there is a lack of hardware emulation platforms for PCLCS. In this demonstration, we present a novel *physiological emulation platform (PEP)* using a hardware-in-the-loop method developed to connect a computational model of the patient's physiology to the actual PCLC device hardware, enabling real-time testing of the device while incorporating the hardware components.

Keywords: hardware emulation · test platform · physiological closed-loop control systems (PCLCS)

1 Introduction and Motivation

Over the last few years, the quality and access to medical care have seen unprecedented improvements, stimulating a revived interest in clinical automation and pushing scientists to develop creative solutions in the domain of physiological closed-loop control systems (PCLCS). A wide variety of experts are striving to generate cutting-edge PCLC-based medical devices and setting up an integrated academic-commercial infrastructure to serve this quickly progressing domain. Given the potential advantages of PCLCS, such as reliable and efficient treatments and the ability to augment medical assistance, especially in emergencies, it becomes crucial to prioritize patient safety in evaluating these systems. The

D. Puthal et al. (Eds.): IFIPIoT 2023, IFIP AICT 684, pp. 410–417, 2024.
https://doi.org/10.1007/978-3-031-45882-8_30

authors in [5] explored the security threats and attacks and the challenges associated with wearable and implantable medical devices (WIMDs) and closed-loop medical control systems.

Automated closed-loop insulin delivery, also known as the artificial pancreas system (APS), is a type of PCLCS that incorporates a continuous glucose sensor, insulin pump, and control algorithm to regulate insulin delivery based on real-time blood glucose values [3]. A well-functioning APS can provide numerous benefits to patients; however, a malfunctioning APS can lead to an overdose or underdose of insulin, putting the patient in danger. A study was conducted to investigate the safety and design requirements of the APS, focusing on both individual components and the system as a whole [1]. The US Food and Drug Administration (FDA) emphasizes the importance of ensuring the safety and reliability of PCLCS since malfunctioning medical devices can lead to severe injury or even death [2].

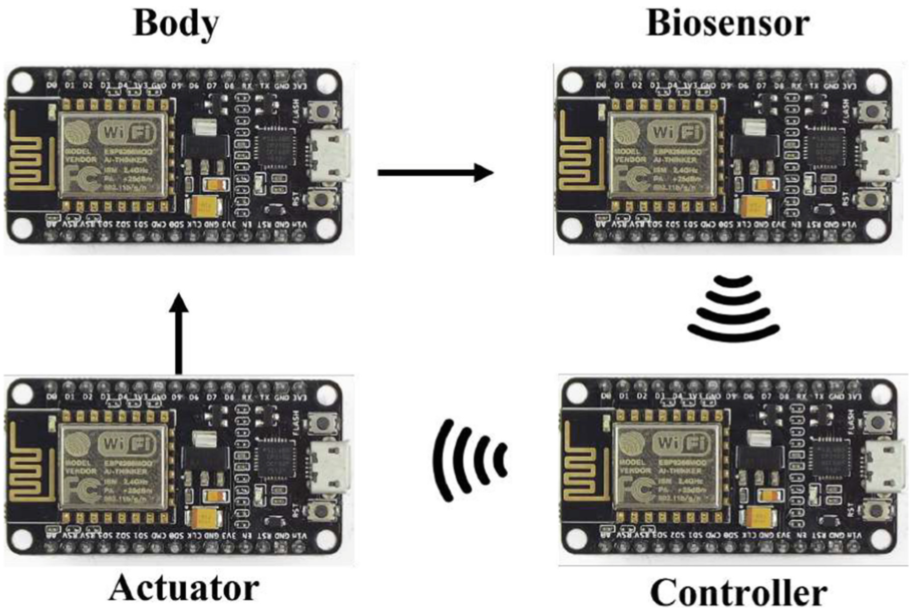


Fig. 1. Overview of our emulation platform showing the connectivity between the different hardware components.

Evaluating the functionality and safety of PCLCS in every relevant clinical scenario through animal and human trials is not practical due to the complexity of these systems and the potential for various disturbances to affect their operation. As a result, closed-loop systems in various engineering fields are typically designed through computational and mathematical modeling to increase efficiency, reduce costs, and avoid errors during the development process. This approach of evaluating PCLCS through a computational or mathematical model of the patient response can provide a complementary or alternative solution to traditional animal and clinical studies [2]. The development of hardware-in-the-loop testing platforms has been driven by the need for a more efficient alternative to costly and resource-intensive clinical trials. As a result, the focus has been on systems that impact the most vital organs, such as heart testbeds for the validation of pacemakers [4] and cardiovascular interventions [9], and robotic surgery testbeds for MRI-guided biopsy [7]. In recent years, there have been significant developments in the area of *in silico* trials for insulin control algorithms aimed at promoting research on APS [8]. Furthermore, the authors in [10] present a novel and open-source testbed for APS, which includes realistic controllers, simulations of a broad range of patient profiles, and a simulation of potential adverse events. Despite the presence of various software simulation platforms that can model certain physiological systems, there is currently a shortage of *hardware emulation platforms* for PCLCS. The creation of such a platform could provide a vast amount of data that can be further analyzed to enhance the safety and reliability of PCLCS. The overview of our emulation platform is shown in Fig. 1, which displays the connectivity between the different hardware components.

In this research demonstration, we present a platform using a hardware-in-the-loop method that can connect a computational model of the patient's physiology to the actual PCLC device hardware, enabling real-time testing of the device while incorporating the hardware components. The main contributions are as follows:

1. We develop PEP, a novel *hardware emulation platform* comprised of all the major PCLCS components to serve as a reliable tool for testing and optimizing closed-loop medical control systems.
2. We simulate APS as a case study and demonstrate the emulator's effectiveness and functionality, which provides a comprehensive assessment of its ability to accurately mimic the physiological system's behavior.

2 Proposed Design

We developed a hardware emulation platform, PEP that consists of four modules: (1) body; (2) sensor; (3) controller; and (4) actuator. In this section, we will discuss the implementation details of each module, which collectively simulate an APS. Figure 2 illustrates the experimental setup of PEP, emphasizing the individual modules comprising the platform. The modules are based on the ESP8266 development kit, which features a 32-bit microprocessor using the Tensilica Diamond Standard 80 MHZ CPU. It has 17 GPIO pins and supports I2C, UART, and SPI buses. The ESP8266 also includes built-in wireless capabilities with a 2.4 GHz antenna, and deep sleep operating features, making it ideal for IoMT projects. The current system has the capability to emulate three distinct patient types: adult, adolescent, and child. Upon startup, the user can select the desired patient type from a menu screen displayed on an OLED I2C display. The patient data used for emulation is sourced from an average of 100 in silico adults, adolescents, and children, as detailed in [6]. It is worth noting that our system is flexible and can readily support other types of patients as needed.

2.1 Body

The body module replicates essential processes within the human body, such as blood glucose concentration. To generate glucose signals, a control algorithm based on glucose kinematics differential equations obtained from the UVA/PADOVA simulator [6] is employed. These signals are transmitted through a serial bus (UART) to and from the biosensor and controller module. A push-button is utilized as input through a dedicated receiving GPIO pin to mimic the effect of a meal. By modifying the biosignals based on inputs from the controller module, the platform emulates the dynamic behavior of an actual PCLCS.

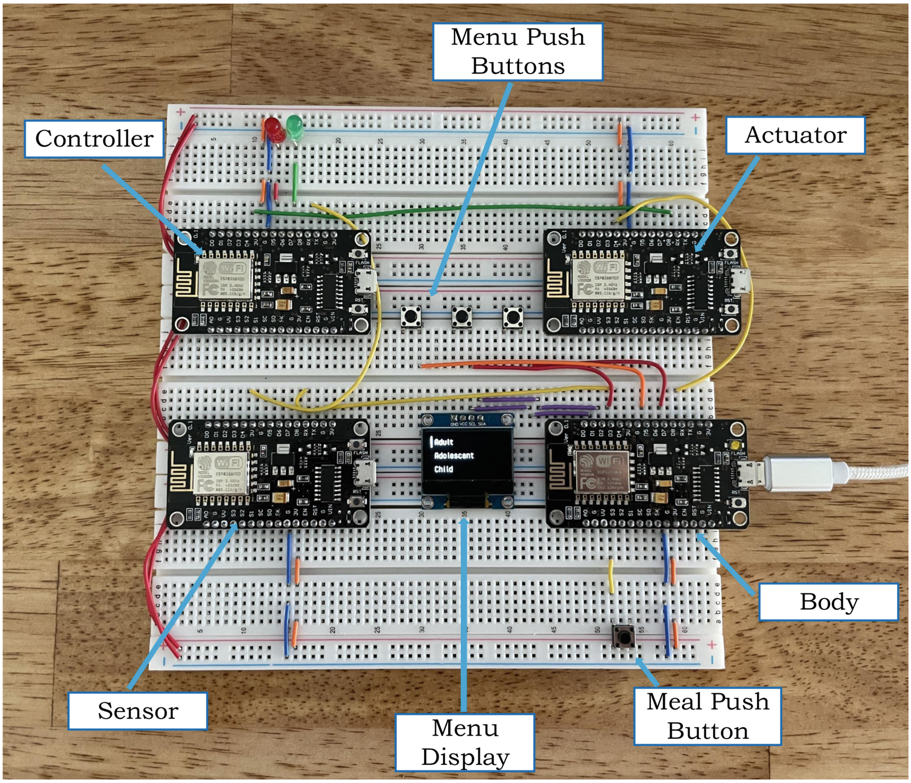


Fig. 2. Experimental setup of the proposed hardware emulation platform, *PEP*.

2.2 Sensor

The sensor module receives input data from the body module via a wired connection. The biosignals captured by the sensor module are then transmitted to the controller module through Wi-Fi, utilizing a client-server model with HTTP requests. This wireless transmission enables seamless communication between the modules, facilitating real-time data exchange. As a backup, the sensor is also connected to the controller via the UART bus, allowing for both wired and wireless testing methods.

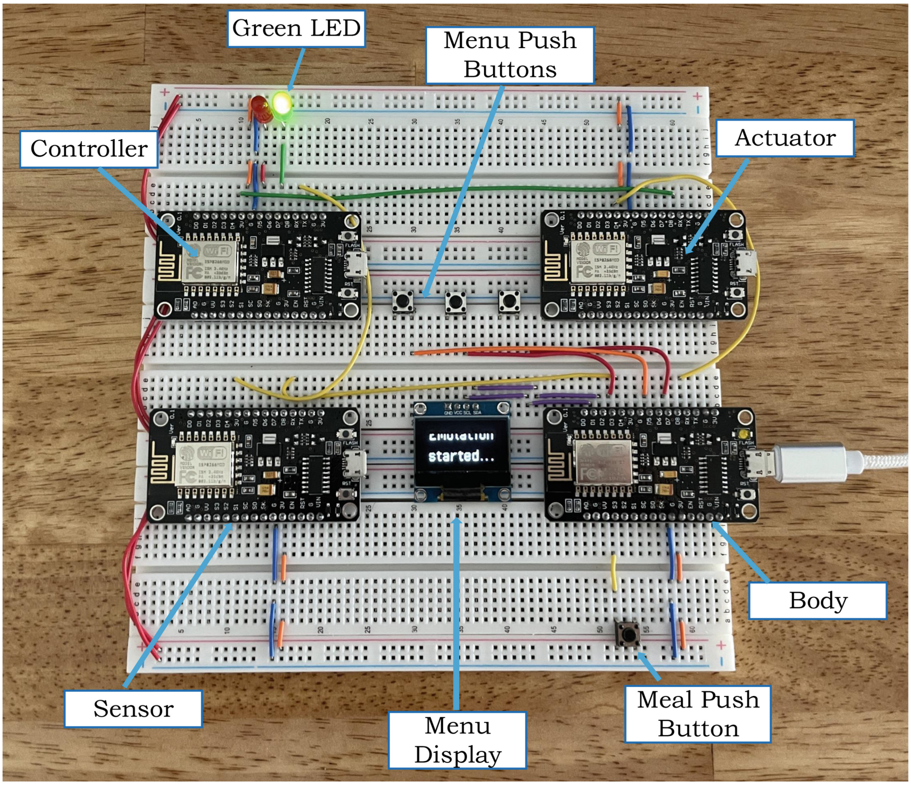


Fig. 3. PEP with a green led indicating a normal range of the measured glucose value. (Color figure online)

2.3 Controller

Within the controller module, wireless input data is received from the sensor module. The controller module uses a control algorithm to calculate the appropriate therapy or treatment required. The calculations are based on the glucose kinematics differential equations. Once determined, the treatment amount is sent to the actuator module via Wi-Fi employing a client-server model with HTTP requests, or through a wired UART bus. The controller module also incorporates an alert system featuring green and red LEDs. These LEDs indicate normal and out-of-range glucose values, providing visual feedback to the user.

2.4 Actuator

The actuator module receives wireless input from the controller module and applies the necessary treatment to the body through wired connections. Based on the calculated treatment amount, the actuator module administers insulin or glucagon, aiming to maintain the physiological parameters within the desired range.

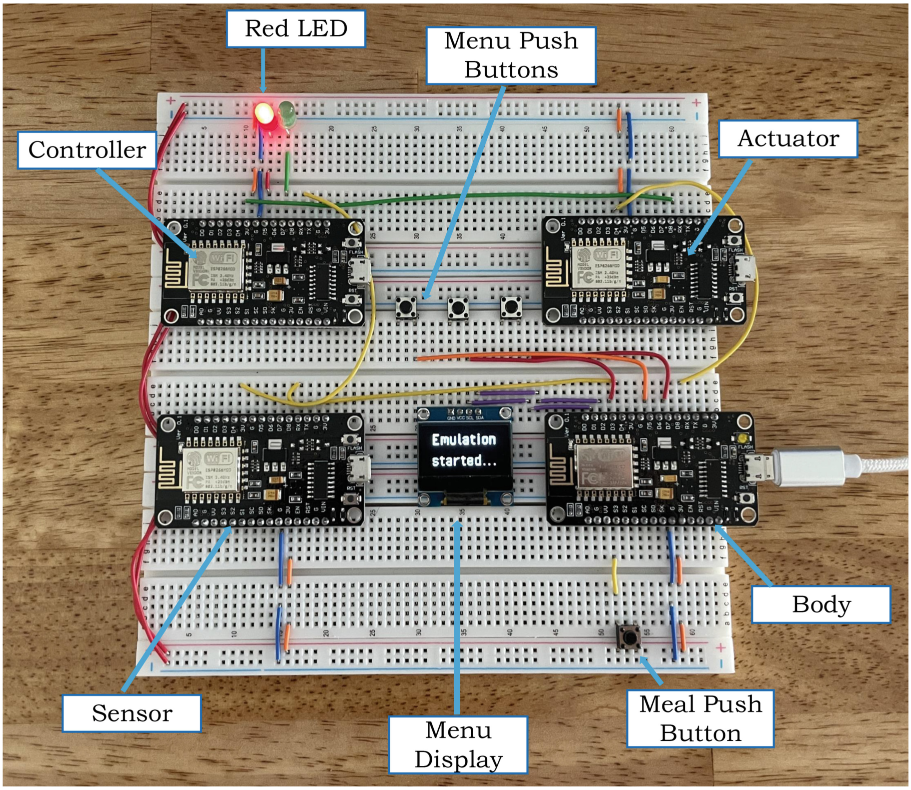


Fig. 4. PEP with a red LED indicating that the measured glucose value is out-of-range. (Color figure online)

3 Experimental Results and Discussion

In this section, we present two figures that demonstrate the accuracy of PEP in indicating normal or out-of-range glucose values. Figure 3 shows a green LED, indicating that the measured glucose value is within the normal range. Figure 4 displays a red LED to highlight that the measured glucose value is outside the normal range, specifically, below 70 or above 180.

The PEP offers a versatile foundation for modeling various faults or attacks, considering the overall system and individual components. The sensor module can be configured through precise programming to replicate diverse issues, including sensor drift or defective acquisition circuits. Additionally, the controller within the PEP allows for the simulation of various faults or malicious attacks, such as denial of service (DoS) or communication prevention. By leveraging the capabilities of the PEP, the actuator can also be effectively modeled to mimic incorrect treatment scenarios, providing valuable insights into potential vulnerabilities or weaknesses in the medical system. This comprehensive fault and attack modeling capacity enables researchers and developers to conduct in-depth testing and assessment of the system's robustness and resilience against potential real-world challenges. Furthermore, the PEP's adaptability facilitates the examination of component-specific faults, enabling a granular analysis of individual modules within the medical system. Researchers can delve into the complex interplay between various components and evaluate the system's response to faults or attacks at different levels, paving the way for precise identification and resolution of weaknesses.

Overall, the PEP can be an indispensable tool for enhancing the security and reliability of closed-loop medical control systems, providing an invaluable testing platform for designing and reinforcing systems against potential faults and malicious intrusions. Its multifaceted capabilities can be utilized to optimize medical systems, ensuring their resilience and trustworthiness in real-world scenarios, ultimately contributing to safer and more efficient patient care.

4 Conclusion

In this research demonstration, we introduced the physiological emulation platform, PEP, a versatile hardware emulation platform capable of replicating the behavior of any physiological system. As a case study, we utilized PEP to simulate an Artificial Pancreas System (APS), showcasing its ability to effectively emulate the APS's functionality. By modeling various physiological responses and system components, PEP can serve as a valuable tool for assessing the security and reliability of PCLCS in different scenarios. Future work will involve expanding the platform to include modeling and evaluating different types of faults or attacks targeting individual system modules. This extension will enable comprehensive security analyses and help designers develop more robust and secure PCLCS in the evolving landscape of modern healthcare applications.

References

1. Blauw, H., Keith-Hynes, P., Koops, R., DeVries, J.H.: A review of safety and design requirements of the artificial pancreas. Ann. Biomed. Eng. **44**(11), 3158–3172 (2016)
2. FDA-Guidelines: Technical considerations for medical devices with physiologic closed-loop control technology. https://www.fda.gov/regulatory-information/search-fda-guidance-documents/technical-considerations-medical-devices-physiologic-closed-loop-control-technology(2021) Accessed 06-Feb 2023
3. Hovorka, R.: Closed-loop insulin delivery: from bench to clinical practice. Nat. Rev. Endocrinol. **7**(7), 385–395 (2011)
4. Jiang, Z., Connolly, A., Mangharam, R.: Using the virtual heart model to validate the mode-switch pacemaker operation. In: Annual International Conference of the IEEE Engineering in Medicine and Biology. IEEE, pp. 6690–6693 (2010)
5. Mahmud, S., Zareen, F., Olney, B., Karam, R., et al.: Trojan resilience in implantable and wearable medical devices with virtual biosensing. In: 2022 IEEE 40th International Conference on Computer Design (ICCD), IEEE, pp. 577–584 (2022)
6. Man, C.D., Micheletto, F., Lv, D., Breton, M., Kovatchev, B., Cobelli, C.: The uva/padova type 1 diabetes simulator: new features. J. Diabetes Sci. Technol. **8**(1), 26–34 (2014)
7. Mendoza, E., Whitney, J.P.: A testbed for haptic and magnetic resonance imaging-guided percutaneous needle biopsy. IEEE Robot. Autom. Lett. **4**(4), 3177–3183 (2019)
8. Schmitzer, J., Strobel, C., Blechschmidt, R., Tappe, A., Peuscher, H.: Efficient closed loop simulation of do-it-yourself artificial pancreas systems. J. Diabetes Sci. Technol. **16**(1), 61–69 (2022)
9. Vrooijink, G.J., Irzan, H., Misra, S.: A beating heart testbed for the evaluation of robotic cardiovascular interventions. In: 2018 7th IEEE International Conference on Biomedical Robotics and Biomechatronics (Biorob), IEEE, pp. 1076–1082 (2018)
10. Zhou, X., Kouzel, M., Ren, H., Alemzadeh, H.: Design and validation of an open-source closed-loop testbed for artificial pancreas systems. In: 2022 IEEE/ACM Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE), IEEE, pp. 1–12 (2022)

Author Index

Published by Springer Nature Switzerland AG 2024
D. Puthal et al. (Eds.): IFIPIoT 2023, IFIP AICT 684, pp. 419–421, 2024.
https://doi.org/10.1007/978-3-031-45882-8